

**DATE:** March 31, 2004  
**ACTION:** FEDSIM Redirects SAIC's Training Resources from WBT to ILT  
**IMPACT:** REQUIREMENTS (redirect)

Government requested SAIC to redirect resources to support Instructor-Led-Training (ILT) as a higher priority than those activities necessary to continue developing the remaining 37 "Detailed" Web Based Training (WBT) lessons (per completion of the remaining four lessons of the 16 WBT "Overview" lessons).

**DATE:** April 6, 2004  
**ACTION:** FEDSIM Issues Second Extension to ETC Deadline (w/ Gov expectations)  
**IMPACT:** COST  
SCHEDULE  
REQUIREMENTS  
CONFIDENCE

The ETC deadline was granted a second extension. Deadline was extended to April 14, 2004. In granting this extension, Government expectations with the ETC were communicated as follows:

- ETC proposal would be final, accurate and complete with respect to activities and costs associated with completing the UAC project.
- ETC would demonstrate how SAIC intended to get the program back on track with respect to performance, schedule and cost management.
- ETC process needed to boost Government confidence in SAIC's ability to complete this critical program.

**DATE:** April 14, 2004  
**ACTION:** Contractor's ETC Received  
**IMPACT:** COST  
SCHEDULE  
REQUIREMENTS

Contractor provided ETC cost and technical proposal for the Trilogy UAC program in its entirety (projected to end September, 2005).

ETC Submission reflected the following data:

- Provided plan for completion of Delivery 1 including new work
- Maintained flash cutover approach as previously directed
- Budgetary estimates for requested options (5 options total)

Increase in CLIN 0001 (Labor) with this ETC submission approximately: \$56.5M

Schedule:

1. July 13 '04: Software complete, ready for final testing
2. Aug 31 '04: Preliminary (dry run) System Acceptance Test (SAT) complete
3. Nov 10 '04: SAT complete (last 2 weeks reserved for final regression testing)
4. Dec 17 '04: Data migration complete
5. Dec 30 '04: Deployment complete

Key Items:

- Records Management Application (RMA) and FIF/SAR Reporting developed and implemented separately
  - RMA implementation drove schedule an additional 4 months out

- FIF/SAR reporting (separated from ingest) also would drive out the software complete milestone
- All test cases need to include a Gov approval prior to start of SAT
- Functional changes need to be frozen as of March 22 '04
- Acceptance test criteria are assumed to be equivalent to System Test acceptance criteria
  - Formal documentation that defines Acceptance Criteria needed by May 10, '04

<b>DATE:</b>	April 21, 2004
<b>ACTION:</b>	SAIC Briefs Government on ETC Proposal and Alternatives
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS CONFIDENCE (failed to meet Gov expectations)

- SAIC briefed the Government at JEH on April 21 on the proposed ETC plan.
- SAIC also presented 3 alternative approaches to the Government with intent to reduce schedule for Delivery 1 and reduce deployment risk:
  - **Alternative #1:** System Test and Deferred Data Migration with System ready for use in October 2004
  - **Alternative #2:** Incremental Deployment
  - **Alternative #3:** Incremental Deployment with Operational Assessment with Initial System Use in September 2004

**SAIC failed to meet Government expectations with the ETC briefing as well as the proposed alternative approaches due to the following positions cited by the Government:**

- SAIC failed to address what was requested via the FEDSIM April 4, 2004 letter (2<sup>nd</sup> extension to ETC): "The ETC will address how SAIC intends to get this project back on track with respect to performance, schedule and cost management in order to boost the Government's confidence in the ETC as well as SAIC's ability to complete this critical project."
- ETC and alternatives contained unacceptable and unreasonable assumptions, qualifications and risks
- SAIC failed to identify technical leadership
- SAIC failed to identify a realistic plan to get the Government to D1

<b>DATE:</b>	May 3, 2004
<b>ACTION:</b>	- FEDSIM directs SAIC to suspend all Instructor-Led-Training (ILT) activities
<b>IMPACT:</b>	- FEDSIM redirects SAIC's training resources back to WBT (from ILT) COST SCHEDULE REQUIREMENTS (redirect/stop work)

- SAIC was directed to suspend work on all development and related activities recognized in the Government approved Change Request (CR) 500 for Instructor-Led-Training (ILT).

- The Government redirected SAIC to resume the Web based training (WBT) lesson activities immediately as set forth in ECP01b for WBT development.

<b>DATE:</b>	May 4, 2004
<b>ACTION:</b>	FEDSIM directs SAIC to Stop all Consent-to-Purchase (CTP) activities
<b>IMPACT:</b>	COST (shut down tool purchases) SCHEDULE REQUIREMENTS

FEDSIM's written correspondence to SAIC to stop all CTP activities resulted from an internal FBI directive to the VCF team and Finance Department to freeze/stop all CTP expenditures as of April 29, 2004.

<b>DATE:</b>	May 14, 2004
<b>ACTION:</b>	FEDSIM Requests 3 Decision Documents From SAIC
<b>IMPACT:</b>	COST (add additional funding to continue program OR not) SCHEDULE (extend PoP to continue program OR not) REQUIREMENTS (meeting expectations OR not) RELATIONSHIP (continue OR end)

Pending Government determinations (including the decision to continue with SAIC or not) required further information from the Contractor. As such, the Government requested the following documentation from SAIC:

1. SAIC Provisional Program Plan, to include the items for Initial Operating Capability (IOC) as communicated in SAIC's May 14 email correspondence to the FBI
2. Design Document(s)  
(The Government anticipated final submittals to capture revisions reflecting previously documented FBI/Mitretek comments and concerns.)
3. Results of the performance characterization testing conducted at the Clarksburg facility

Deadline for the above decision documentation was set for May 21, 2004.

In order for a decision to be made that would be in the best interest of the Government, the above pertinent information was required by May 21 in order to prevent SAIC from operating at risk beyond SAIC's stated date of June 17, 2004 for depletion of funds for CLIN 0001 (Labor).

This was also to prevent further cost accruals should the Government choose not to provide further funding (i.e. let the funding contract run out/let the contract end - NOT TO BE MISINTERPRETED as a contractual action of "Termination").

Per the above schedule and cost constraints, decision documents were to be submitted "as-is" regardless of document state (finalized form or not).

<b>DATE:</b>	May 19, 2004
<b>ACTION:</b>	FEDSIM Requests VCF Shut Down Estimates (Costs)
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

FEDSIM requested SAIC to provide an estimate of costs associated with shutting down the VCF program. Modification PA26 changes the FBI TPOC to Joseph Brandon.

Shutdown estimates/projected costs deadline was set for May 25, 2004.

<b>DATE:</b>	May 20, 2004
<b>ACTION:</b>	FEDSIM Deems SAIC ETC Unacceptable
<b>IMPACT:</b>	COST (unacceptable to commit additional funds) SCHEDULE (unacceptable to extend PoP) REQUIREMENTS (unacceptable) CONFIDENCE (failed to meet Gov expectations)

FEDSIM notified SAIC that per Government review of the ETC dated April 14, 2004, the ETC was deemed unacceptable.

The Government's evaluation of the ETC package determined that the ETC was inadequate, failed to meet expectations, and did not contain the level of detail required for the FBI to make a decision regarding extending the period of performance against a new cost and schedule baseline for VCF deployment.

<b>DATE:</b>	May 20, 2004
<b>ACTION:</b>	FEDSIM Requests Provisional Program Plan (Initial NOT Full Capability)
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (redirect/descope) - Intent to redirect contractor towards IOC responsibilities ONLY - Intent to remove FOC responsibilities from contractor

Driven by Government concerns regarding contractor performance and capabilities, the Government now focused on providing contractor direction that would ONLY address an Initial Operating Capability (IOC) of VCF core capabilities (to be defined) that MUST be deployed by December '04.

Again, driven by Government concerns regarding contractor performance and capabilities, Government intent was now to remove VCF responsibilities for Full Operating Capability (FOC) from this task order.

FEDSIM forwarded written correspondence to SAIC that identified the following five items/functions as critical functionality that must be included in the Initial Operating Capability (IOC) of the VCF:

- Cases, Leads, and Evidence Requests
- Security Model Enhancements
- Consolidated Logging
- Silent Hits Against Person Objects
- EPAIS Interface

SAIC was directed to address cost, schedule and related dependencies of the above items as they relate to IOC functionality (as discussed in previous joint meetings held among FBI, FEDSIM and SAIC).

Provisional Program deadline was set for May 26, 2004.



<b>DATE:</b>	May 25, 2004
<b>ACTION:</b>	VCF Core Capabilities Vision presented by the Government to SAIC
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (redirect/descope )

The Government presented its own vision of an Initial Operating Capability (IOC) to SAIC at the Mitretek (a Government Support Contractor) Fairview Park facility. Objectives of this gameplan included:

1. Deployment of an operational VCF system in calendar year 2004
2. Deployment of a highly reliable core capability

The Government proposed the following Initial Operating Capability (IOC) approach to SAIC:

- Reduce deployment risk by continuing to use ACS case management capabilities until VCF is proven and ready
- Use VCF workflow capability to create ACS serials, thereby expediting access to new data to all users

The Government proposed the following deployable capabilities to SAIC:

- Leads Management
- Case Management
- Document Management

<b>DATE:</b>	May 25, 2004
<b>ACTION:</b>	SAIC Submits Shut Down Estimates
<b>IMPACT:</b>	COST (shut down estimate) SCHEDULE REQUIREMENTS

SAIC's estimate of costs associated with shutting down and closing of Trilogy UAC project was submitted at \$3.5M.

<b>DATE:</b>	May 25, 2004
<b>ACTION:</b>	FEDSIM Redirects SAIC on Provisional Program Plan
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (redirect/define)

FEDSIM provided revised direction concerning SAIC's submission of the Provisional Program Plan with Initial Operating Capability (IOC) functionality.

FEDSIM requested SAIC NOT to submit a plan at this time as originally directed on May 20 because the FBI was currently reviewing the functionality required of the IOC. Further direction concerning submission of the Provisional Program Plan would be forthcoming.

<b>DATE:</b>	May 26, 2004
<b>ACTION:</b>	SAIC Responds to VCF Core Capabilities Vision presented on May 25
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (redirect/descope)

An all parties (FBI, FEDSIM and SAIC) teleconference was held to allow SAIC to respond to the May 25 Government presentation/vision of the "VCF Core Capabilities" that was briefed for SAIC to consider the Government's alternative approach to achieve deployment of a highly reliable VCF system core capability to be operational in calendar year 2004.

**SAIC Summary Response to the Government proposed IOC approach was documented as follows:**

- "We (SAIC) fully support the IOC/FOC phased approach to implementation - - it is technically feasible and a sound approach for enterprise system deployment."
- "The approach to start with core capability and add requirement modules over time reduces risk and assures that the IOC will be a highly reliable and operationally useful system."
- "The details and nuances of each option needs to be completely understood."
- "With anticipated direction by May 28<sup>th</sup> we (SAIC) are confident that we can have an ETC for the IOC by June 28<sup>th</sup>" - ASSUMING design is frozen on June 14, 2004

<b>DATE:</b>	May 26, 2004
<b>ACTION:</b>	SAIC Briefs the Government on VCF Performance Characterization Test Results
<b>IMPACT:</b>	REQUIREMENTS CONFIDENCE (failed to meet Gov expectations)

SAIC briefed the Government (DOJ, OMB, FBI and FEDSIM) at DOJ Headquarters on Performance Characterization findings regarding the VCF system.

SAIC conducted the briefing with the following SAIC objective: **Determine the ability of the current VCF architecture to meet performance and scalability requirements.**

SAIC's testing plans/processes/criteria had not been approved by the Government for these particular testing activities (SAIC working from proposed/unapproved ETC).

Results provided presented a challenge for the Government to accurately measure and/or quantify any level of success, with any degree of certainty. Again it was SAIC's objective to "determine the ability of the current VCF architecture to meet performance and scalability requirements." With this objective in mind, the briefing failed to quantify any level of confidence that the Government would have to answer to, with accountability and responsibility, in the promoting of, or the defending of, the VCF system.

<b>DATE:</b>	May 28, 2004
<b>ACTION:</b>	SAIC delivers 3 <sup>rd</sup> and final installment of Design documentation
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (failed to meet Gov expectations) CONFIDENCE (failed to meet Gov expectations)

SAIC's Software Design Document, as delivered on May 28, represented the third and final (as of 28 May 04) submittal of the software design and software architecture including information (40 docs in total) regarding hardware, interfaces, performance, database, and security as it relates to the development and design architecture of the VCF application.

Per ongoing FBI/Mitretek review and assessments, design documentation and deliverables provided by SAIC to date have failed to meet Government expectations.

<b>DATE:</b>	June 10, 2004
<b>ACTION:</b>	FEDSIM Directs SAIC to Shut Down NON-IOC Activities
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (stop work/descope) - Redirect contractor towards IOC responsibilities ONLY - Remove FOC responsibilities from contractor

The Government issued a Stop-Work Order to SAIC (effective June 10, 2004) that would affect all activities not specifically related to the IOC functionality (in accordance with the clause at FAR 52.242-15, Stop-Work Order, Alternate I, Apr. 1984). The duration of this Stop-Work order would be 90 days unless otherwise notified by the FEDSIM Contracting Officer.

Activities affected by this order were documented via the following 2 attachments:

- Attachment 1 - Identified those functional areas that would not be operational in IOC (list drafted by the FBI – previously reviewed by SAIC)
- Attachment 2 - Identified those non-IOC activities from the 14 April 04 ETC (list was developed via a 7 June 04 working meeting between SAIC and FBI)
- The Government also requested SAIC to stop work on all data migration activities, with the exception of support for the data migration staging database (normalized version of ACS residing on ORACLE) which would include:
  - Extraction of data from the ACS application to populate the staging database
  - Synchronize data updates between the ACS application and the staging database
  - Analyze data error conditions and provide reports describing these conditions, including level of severity and alternatives for resolution
- The Government also requested SAIC to stop work on all non IOC-related Software Problem Reports (SPRs) and Test Cases (per review and identification activities to clarify any IOC relation).
- The Government also requested SAIC to stop work on the Delivery I Test Plan.
- The Government also requested SAIC to provide a revised estimate of funds expenditure date (revised "burn rate") based on this directive by June 14, 2004.

Finally the Government requested SAIC to forward any concerns if any of the above directives would impact deployment of IOC capability in CY 2004. If so, SAIC was directed to respond to FEDSIM by June 14, 2004 (and before any stop work actions would be implemented).

<b>DATE:</b>	June 14, 2004
<b>ACTION:</b>	SAIC Responds to NON-IOC Shut Down Directive
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

- SAIC letter confirmed that the affected project personnel stopped work on the identified activities as of COB Friday, June 11, 2004.
- SAIC identified two areas of work that should be continued (as captured in their correspondence, verbatim):

"1) **Text Search** - The text search capability modifications identified in November 2003 are nearly complete. The final software updates will be turned over to the VCF integration environment on June 25th. This completes a major re-implementation of the text search capability. It is in the Government's best interest to complete this work at this orderly stopping point to be able to efficiently restart the implementation of text search in the future."

"2) **Performance Engineering** - The IOC implementation requires an appropriate level of performance testing and tuning. Four of the major performance measurement transactions (Login, Import, View Document, and Notifications) are directly relevant to the IOC baseline. Performance testing will be limited to the IOC scope and is less than what was previously required. This work is key to ensuring a robust, reliable baseline that will successfully support peak workloads and continue to meet end user response time requirements."

- SAIC also requested clarification on the direction to continue some elements of the data migration activities.
- SAIC reduced its staff by a total of fifty-five (55) (including subcontractor personnel) as a result of the Stop Work Order. This reduction in staff changed the funds expenditure date to June 18, 2004.

SAIC still required agreement on the IOC capability baseline and acceptance criteria by June 17th, 2004 in order to deliver IOC this calendar year.

<b>DATE:</b>	June 15, 2004
<b>ACTION:</b>	Agreement between Director Mueller and CEO of SAIC
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

- FBI Director reached an agreement with SAIC CEO that recognized an estimated cost of \$17M to complete and deploy VCF IOC by December 31, 2004. This same agreement also recognized specific cost sharing stipulations, as well as an award fee amount of \$2.6M

(pending successful VCF IOC deployment and acceptance), specifics to be subsequently negotiated.

<b>DATE:</b>	June 18, 2004
<b>ACTION:</b>	Modification to realign funding
<b>IMPACT:</b>	COST

- Funding is realigned from travel and ODCs to Labor to reflect decreased requirements for those CLINs and anticipated increase in labor because of program realignment.

<b>DATE:</b>	June 28, 2004
<b>ACTION:</b>	FEDSIM issues RFP to SAIC for VCF IOC
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

- FEDSIM issued an RFP to SAIC for the VCF IOC (only). Applicable sections of the Task Order have been/will be modified as a result of joint "Alpha Contracting" sessions.

<b>DATE:</b>	July 6, 2004
<b>ACTION:</b>	Begin Renegotiation and implementation of Corrective Action Plan (Track I) Alpha Sessions Begin
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

**COST FOR RENEGOTIATED EFFORT (IOC): ESTIMATED \$17m**

**SCHEDULE:**

- |                          |   |              |
|--------------------------|---|--------------|
| • <b>Control Gate 1:</b> | Credible IOC VCF Plan                         | Jul 27, 2004 |
| • <b>Control Gate 2:</b> | Design Review                                 | TBD          |
| • <b>Control Gate 3:</b> | System Acceptance Test Readiness Review (TRR) | TBD          |
| • <b>Control Gate 4:</b> | Operational Readiness Review (ORR)            | TBD          |
| • <b>Deployment:</b>     | Initial Operating Capability (IOC) of the VCF | Dec 31, 2004 |

**TRILOGY UAC ACCOMPLISHMENTS SINCE MARCH 19, 2004:**

- Briefed GAO on Security design in March 2004
- Provided weekly status (Green books) and Periodic Status Reports
- Completed full dry run of data migration in April 2004 (except for documents not released by the FBI)
- Made several organizational changes including Chief Engineer, addition of Dr. Perry, new Software Engineering Manager, new Data Engineering Manager
- Completed Performance Characterization testing and briefed results on May 26, 2004
- Submitted final VCF Design Documents on May 28, 2004
- Defined several options for incremental deployment of VCF during April/May 2004

- Developed VCF IOC definition with the Government from May 26 through June 25, 2004
- Developed ROM engineering estimates for the IOC May 29-31
- Participated in pre-Alpha contracting sessions to develop the Statement of work, acceptance criteria, and requirements from June 21 through July 2, 2004
- Supported IV&V of IOC Definition document and Functional Descriptions/Scenarios on June 30, 2004

**DISPOSITION:**

The Alpha Contracting sessions began Tuesday, July 6, 2004 at SAIC's Vienna facility. The sessions are scheduled to last three weeks (through July 27). Sessions will include review, discussion, negotiation and agreement to Basis of Estimates (BOEs), Work Breakdown Structure (WBS), Resource Loaded Network (RLN) and all other supporting documentation of SAIC's cost, schedule and technical approach to VCF IOC.

The Government anticipates reaching full agreement/closure on the VCF IOC modification by July 27, 2004 (the projected exit date for Control Gate 1) so that additional funds may be added to the contract in a timely manner.

GSA, through this task order with SAIC, is committed to provide the FBI with a successful VCF IOC solution that meets all applicable VCF IOC requirements. GSA will continue to work as a team with both the FBI and SAIC to bring the Trilogy VCF IOC task to a successful completion.

<b>DATE:</b>	July 29, 2004
<b>ACTION:</b>	Modification PS28
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

- Modification incorporates initial IOC agreement as a result of alpha sessions to include:
  - Reduce existing award fee ceiling of \$7,052,566 and make those funds available for labor; no award fee will be paid as part of the IOC effort.
  - Incorporate "Control Gate" concept

<b>DATE:</b>	July 29, 2004
<b>ACTION:</b>	Modification PS29
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

- Bilateral modification incorporates all of the IOC agreement, including cost sharing, revised Statement of Work descopeing the effort to ONLY IOC. Total value of renegotiated order is \$126,973,479, of which \$17 million is the cost for the IOC. SAIC will contribute \$5.6 million towards the estimated cost of \$17 million for IOC. If the IOC is deployed on time and under the estimated cost, then SAIC will be entitled to a rebate of \$2.6 million of it contribution. Net cost sharing if successful: 83% Government/17% Contractor.
- Control Gate One achieved

**DATE:** August 23, 2004  
**ACTION:** Modification PO30  
**IMPACT:** COST

- Provide incremental funding.

**DATE:** 30 September, 2004  
**ACTION:** Modification PS31  
**IMPACT:** NONE

- Modification to incorporate revised Section F deliverable dates. No impact to overall schedule

**DATE:** 6 October, 2004  
**ACTION:** Control Gate 2 Achieved  
**IMPACT:** COST  
SCHEDULE  
REQUIREMENTS

**DATE:** October 21, 2004  
**ACTION:** Modification PO32  
**IMPACT:** COST

- Provide incremental funding

**DATE:** November 6, 2004  
**ACTION:** Modification PS33  
**IMPACT:** COST  
SCHEDULE  
REQUIREMENTS

- Control Gate 3 achieved on schedule, currently running at about \$2.4 million under estimated costs.
- Provide incremental funding
- FBI chooses to exercise post deployment support options for enhanced IOC capabilities (IOC Plus) and operations and maintenance support
- Total task order value is increased to \$132,167,640

**DATE:** December 16, 2004  
**ACTION:** Modification PO34  
**IMPACT:** COST  
SCHEDULE

- Provide incremental funding
- Incorporate revised (downward) pricing for O&M support. Total task order value is decreased to \$130,293,207 due to changes in level of effort required by FBI for O&M support

**DATE:** 22 December, 2004  
**ACTION:** Modification PO35  
**IMPACT:** COST  
SCHEDULE  
REQUIREMENTS

- Control Gate 4 achieved slightly ahead of schedule, currently running at about \$3.2 million under estimated costs.
- Provide incremental funding

<b>DATE:</b>	17 January 2005
<b>ACTION:</b>	Modification PO36
<b>IMPACT:</b>	COST

- Provide incremental funding

#### **LIVE DOCUMENT NOTE**

This product is a "live" document that exists to capture and provide an ongoing objective historical account of the FBI TRILOGY UAC Task order in order to clearly demonstrate justification for ALL significant contractual actions and directions that have been executed by GSA FEDSIM to date on behalf of its client, the FBI.





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

Office of the Assistant Attorney General

Washington, D.C. 20530

January 3, 2006

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

Dear Mr. Chairman:

Enclosed please find responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on July 27, 2005. The subject of the Committee's hearing was oversight of the Federal Bureau of Investigation.

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

Sincerely,

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

William E. Moschella  
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy  
Ranking Minority Member

EFF Section 215-425

**Responses of the Federal Bureau of Investigation  
Based Upon the July 27, 2005 Hearing Before the  
Senate Committee on the Judiciary  
Regarding FBI Oversight**

**Questions Posed by Senator Specter**

1. Larry Johnson, a former counter-terrorism official at the State Department, said in a July 16, 2005 issue of the National Journal that the FBI is on its sixth counter-terrorism chief since 2001, "There is a rhetorical gap the size of the Grand Canyon, in which the Bush Administration on one hand insists that fighting terrorism is the No. 1 priority, and yet as far as personnel goes, it is treated as the last priority."

a. List the names of each of the FBI counter-terrorism chiefs, with their dates of service in this position and the reasons for their departure. Include as an attachment to this response all internal documents that set forth the reasons for the departure including, but not limited to, employment records. Provide a résumé, curriculum vitae or biography of each of the persons who held this position.

**Response:**

Following are the assignment histories of each Assistant Director (AD) of the FBI's Counterterrorism Division (CTD). Please note that before 11/21/1999, counterterrorism (CT) was part of the National Security Division, which became the Counterintelligence Division (CD) following an FBI reorganization (these assignments are referred to below as assignments to the CD).

**Dale L. Watson**

Entered on duty as a Special Agent (SA) on 2/12/78.

Assigned to Birmingham Division on 5/20/78.

Reassigned to New York on 10/19/82.

Reassigned to CD, FBI Headquarters (FBIHQ) on 1/6/85.

Promoted to Supervisory Special Agent (SSA), CD, on 1/19/86.

Reassigned to Washington Field Office (WFO) on 3/11/87.

Promoted to Unit Chief (UC) in the Criminal Investigative Division (CID) on 11/25/91.

Reassigned to CD UC on 4/23/92.

Promoted to Assistant Special Agent in Charge (ASAC), Kansas City Division, on 5/3/94.

Reassigned to CD as a GS-15 SSA on 9/1/96 and detailed to the National Security Agency.

Promoted to Section Chief (SC), CD, on 12/13/96.

Promoted to Deputy Assistant Director (DAD), CD, on 7/8/98.  
Promoted to AD, CTD, on 12/14/99.  
Promoted to Executive Assistant Director (EAD), CT/Counterintelligence (CI), on  
12/2/01.  
Retired on 9/30/02.

**Pasquale J. D'Amuro**

Entered on duty as an SA on 5/6/79.  
Assigned to the New York Division on 8/22/79.  
Promoted to SSA on 2/15/87.  
Assigned as Assistant Inspector, Inspection Division, on 4/30/95.  
Promoted to GS-15 SSA, CID, on 7/8/96.  
Reassigned as ASAC-CT, New York Division, on 8/31/97.  
Promoted to Associate SAC, New York Division, on 1/29/01.  
Promoted to AD, CTD, on 1/29/02.  
Promoted to EAD, CT/CI, on 11/14/02.  
Reassigned as Assistant Director in Charge (ADIC), New York Division, on  
8/4/03.  
Retired on 3/31/05.

**Larry A. Mefford**

Entered on duty as an SA on 8/6/79.  
Reassigned to Sacramento Division on 11/23/79.  
Reassigned to Los Angeles Division on 9/15/80.  
Reassigned to WFO on 12/21/86.  
Reassigned to the Critical Incident Response Group on 9/27/87.  
Promoted to SSA, CID, on 11/5/89.  
Reassigned to Minneapolis Division on 4/6/92.  
Reassigned to San Francisco Division as an SA on 7/9/95.  
Promoted to SSA, San Francisco Division, on 5/11/97.  
Promoted to ASAC, San Diego Division, on 9/27/98.  
Promoted to Associate SAC, San Francisco Division, on 6/12/00.  
Promoted to AD, Cyber Division (CyD), on 5/28/02.  
Reassigned as AD, CTD, on 11/22/02.  
Promoted to EAD, CT/CI, on 8/18/03.  
Retired on 10/31/03.

**John S. Pistole**

Entered on duty as an SA on 9/18/83.  
Assigned to Minneapolis Division on 1/6/84.  
Reassigned to New York Division on 4/7/86.  
Promoted to SSA, CID, on 11/30/90.

Reassigned to Indianapolis Division on 3/21/94.  
Promoted to ASAC, Boston Division, on 7/4/99.  
Promoted to Inspector on 7/23/01.  
Promoted to DAD, CTD, on 6/3/02.  
Promoted to AD, CTD, on 9/16/03.  
Promoted to EAD, CT/CI, on 12/22/03.  
Promoted to Deputy Director on 10/3/04 (current position).

**Gary M. Bald**

Entered on duty on 9/11/77 and assigned to the Criminal Justice Information Services (CJIS) Division as a fingerprint examiner.  
Reassigned to the Laboratory Division as a physical science aid on 4/24/78.  
Promoted to cryptanalyst on 10/23/78.  
Became an SA on 4/19/81.  
Assigned to Albany Division on 8/10/81.  
Reassigned to Philadelphia Division on 3/31/84.  
Promoted to SSA, Inspection Division, on 6/4/89.  
Reassigned to Newark Division on 8/9/91.  
Promoted to GS-15 Assistant Inspector, Inspection Division, on 4/16/95.  
Reassigned as UC, CID, on 9/3/96.  
Promoted to ASAC, Atlanta Division, on 12/2/96.  
Reassigned as Inspector-in-Charge on 2/25/00.  
Promoted to SAC, Baltimore Division, on 9/30/02.  
Promoted to DAD, CTD, on 11/17/03.  
Promoted to AD, CTD, on 3/4/04.  
Promoted to EAD, CT/CI, on 11/2/04 (current position).

**Willie T. Hulon**

Entered on duty as an SA on 9/6/83.  
Assigned to Mobile Division on 12/22/83.  
Reassigned to Chicago Division on 1/28/86.  
Reassigned to San Antonio Division on 4/11/88.  
Promoted to SSA, San Antonio Division, on 10/20/91.  
Reassigned to CID on 3/19/95.  
Promoted to GS-15 Assistant Inspector, Inspection Division, on 2/4/96.  
Reassigned as UC, CID, on 6/2/97.  
Promoted to ASAC, St. Louis Division, on 3/9/98.  
Promoted to Inspector on 11/3/00.  
Promoted to Chief Inspector on 7/26/01.  
Promoted to SAC, Detroit Division, on 12/3/02.  
Promoted to DAD, CTD, on 6/7/04.  
Promoted to AD, CTD, on 12/26/04 (current position).

b. Provide a statistical report of the number and percentage of FBI human resources assigned solely and entirely to the Counter-Terrorism Division of the FBI.

Response:

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

2. How much of the FBI's resources are dedicated to intelligence, as opposed to prosecutorial, work?

a. What percent of your human resources are assigned full-time to intelligence gathering as opposed to the prosecutorial support role?

Response:

Intelligence is integrated into all aspects of the FBI's law enforcement mission, and is both an investigative tool and a mission unto itself. Intelligence is also a key objective that is pursued during the prosecutorial phase of an investigation. For this reason, it is difficult to answer this question without a clear context. The resources devoted to intelligence as a mission in and of itself (as opposed to intelligence used and produced in the context of an investigative mission) fall; as an accounting matter, within the FBI's Intelligence Decision Unit (IDU). Of the positions included in the FBI's Fiscal Year (FY) 2005 Congressional appropriation (including the FY 2005 supplemental), 15.5 percent are included in the IDU. These positions include the staff assigned to the Directorate of Intelligence (DI) and personnel under the programmatic control of the EAD for Intelligence (EAD-I), as well as a pro rata share of operational, investigative, management, and other support personnel (such as finance, human resources, and legal personnel) who support the intelligence mission.

We stress, however, that no neat dividing lines distinguish intelligence from law enforcement activities. Intelligence is a core investigative tool, and a valuable product of the prosecutorial phase of an investigation.

b. What is the number of full-time equivalents (FTEs) in Intelligence?

Response:

The FBI's FY 2005 Congressional appropriation included 4,365 full-time equivalents in the IDU.

c. What percent of your monetary resources are used in intelligence?

Response:

16.5 percent of the FBI's FY 2005 Congressional appropriation (including the FY 2005 supplemental) is included in the IDU.

3. Director Mueller stated in a recent speech: "The development of the National Security Service ("NSS") is the next step in the evolution of our ability to protect the American public."

a. What plans, policies and strategies has FBI implemented toward this goal?

Response:

The FBI will submit its National Security Branch Implementation Plan to the President shortly. This Plan is being coordinated with the Office of the Director of National Intelligence (ODNI), and several issues must be resolved before submission. In response to the President's six specific instructions, the Plan provides statements of principle from which detailed implementation plans will be developed. As articulated in the Plan, the National Security Branch (NSB) will strengthen the FBI's existing capabilities in these areas by combining the CTD, CD, and DI into an integrated service that effectively leverages the assets and abilities of all three entities. The NSB will be headed by an EAD.

b. Set forth the process by which FBI and Director Negroponte will appoint the head of the NSS.

Response:

The President has directed that the head of the NSB be appointed with the concurrence of the Director of National Intelligence (DNI), and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directs that the Attorney General obtain the concurrence of the DNI before appointing an individual to the position of EAD for Intelligence or any successor position created through reorganization. Because the head of the NSB (the EAD-NSB) is the successor to the EAD-Intelligence position, the FBI Director forwarded to the Attorney General his recommendation for appointment to the position of EAD-NSB. Consistent with the IRTPA, the Attorney General sought the concurrence of the DNI before making the appointment.

The FBI Director recommended Gary M. Bald, EAD for CT/CI, for appointment as the EAD-NSB. This recommendation was approved by the Attorney General, and the DNI concurred in the appointment. The Deputy appointed to assist EAD Bald in directing the NSB is Philip Mudd from the Directorate of Operations at the Central Intelligence Agency (CIA).

**4. Joint Terrorism Task Forces (JTTFs) were set up to coordinate counterterrorism activities between the FBI, state and local law enforcement agencies. The 9/11 Commission Staff Report no. 9 (pg. 10) states that most local and state law enforcement representatives to the JTTFs were simply liaisons and did not fill management or investigative positions.**

**a. Are there currently any non-FBI officials in management positions in any JTTFs?**

**Response:**

At the discretion of the ADIC or SAC (while most Field Divisions are led by SACs, very large FBI Field Divisions are led by ADICs), participating agencies that have devoted significant numbers of employees or resources to a Joint Terrorism Task Force (JTTF) may assign supervisory personnel to handle administrative matters for their employees. Presently, the New York JTTF includes the largest number of management level non-FBI officials (a New York Police Department (NYPD) deputy chief, captains, lieutenants, and sergeants). These are not operational management positions, but are instead filled by personnel managers for the 115 NYPD employees assigned to the New York JTTF. Management-level officials are also assigned to many other JTTFs for the same purpose. In addition, each JTTF has an Executive Board that is chaired by the FBI's ADIC or SAC and is composed of senior federal, state, and local law enforcement officials who review the operations of the JTTF and provide input and recommendations as to the JTTF's investigative direction.

**b. If not, why not?**

**Response:**

For command and control purposes, the FBI ADIC or SAC is a JTTF's overall commander and is responsible for the operational and administrative matters directly associated with that Division's JTTF(s). The operational chain of command (in "top down" order) is as follows: ADIC (if applicable), SAC, ASAC, and SSA. Staffing issues are the responsibility of the FBI chain of command, while the SSA, as the JTTF Supervisor, supervises JTTF operational

activities. All JTTF investigations are opened and conducted in conformance with FBI policy.

c. If so, set forth the name, location and position of such non-FBI official.

**Response:**

Although many JTTFs include non-FBI members in management-level positions with respect to members of their organizations, none are in operational management positions. In the largest New York JTTF, as with other large JTTFs, the staff of each operational squad includes an NYPD sergeant who collaborates with the FBI squad supervisor regarding investigative decisions. This collaboration also occurs among more senior managers, where NYPD lieutenants, captains, and higher share decision making with FBI executive managers. This enhances investigative oversight, which contributes to a more effective CT effort. Ultimately, though, the FBI is responsible for ensuring investigations are conducted in accordance with all aspects of federal law, Attorney General Guidelines, and Department of Justice (DOJ) and FBI policy.

d. How many JTTFs exist today and how many FBI personnel are assigned full time to each JTTF?

**Response:**

Currently, the 103 JTTFs are staffed by a total of 3,714 full-time law enforcement officers, including 2,196 FBI SAs, 683 officers from other federal agencies, and 835 state and local law enforcement officers.

5. A July 19, 2005 *New Yorker* article entitled "*Defending the City*" describes the FBI agents assigned to an NYPD counterterrorism center as "young white men ... standing stiffly against a wall."

a. What kind of interaction do you expect from your agents detailed to local counterterrorism centers?

**Response:**

FBI personnel assigned to local or regional CT centers or to Regional Intelligence Centers (RICs) are expected to be fully engaged, along with other federal, state; and local agencies, in accomplishing the center's mission. FBI personnel are assigned to these centers to facilitate an unimpeded flow of information concerning terrorism threats and intelligence between the centers and the JTTFs,



which are the primary operational and investigative arms of the U.S. Government in the war on terrorism. Coordination between regional CT centers, RICs, the FBI's CTD, and other appropriate entities is accomplished through those assigned or detailed to the JTTFs and to Field Intelligence Groups (FIGs).

**b. Does the FBI plan to make the efforts of municipal law enforcement agencies an integrated part of their counterterrorism operations, contrary to what is being reported?**

**Response:**

The FBI currently incorporates the efforts of municipal, state, and other federal agencies in CT operations because it has found that success against terrorism is best achieved through cooperation among federal, state, and local law enforcement and public safety agencies. The FBI formed the JTTFs to maximize interagency cooperation and coordination and to create cohesive units capable of drawing on resources at all government levels in responding to terrorism threats. Currently, the 103 JTTFs are staffed by 3,714 full-time law enforcement officers (including 835 state and local law enforcement officers) and augmented by 1,355 part-time law enforcement officers, including 121 FBI SAs, 708 officers from other federal agencies, and 526 state and local law enforcement officers.

**c. If so, what specific plans does the FBI have to more fully integrate their agents into these centers?**

**Response:**

FBI ADICs and SACs are encouraged to interact with and participate in regional CT centers and RICs in their territories. While there may not be a regional CT center or RIC in every ADIC's or SAC's territory, all FBI field offices currently manage and operate FIGs, which serve as the central intelligence component of every FBI Field Office and perform the office's core intelligence functions. The primary mission of these FIGs, which are predominantly staffed by FBI intelligence analysts (IAs), is to provide direct operational and strategic analytical support to the JTTFs. The FIGs and JTTFs both have roles in ensuring that intelligence collected by the JTTF is properly and timely disseminated to intelligence customers.

d. Has anyone within FBI Headquarters investigated these assertions made in the *New Yorker* article and has any corrective action been taken?

Response:

While the FBI is aware of this article, no changes or adjustments to the FBI's operating procedures have been made as a direct result of the claims made in the article.

6. The FBI often seems reluctant to share pertinent information with local and state law enforcement agencies. The *New Yorker* article cites an instance in October 2001 when the White House was informed that a 10-kiloton nuclear weapon was being smuggled into New York City (p. 61). Mayor Giuliani and the NYPD were not informed of this threat. Today, the NYPD complains that while the flow of information has improved, integrated intelligence sharing does not yet occur. What is the FBI doing to actively improve the flow of terrorism information between the FBI and state and local law enforcement agencies?

Response:

The FBI takes such criticisms very seriously and is implementing a three-pronged strategy to improve the flow of information through policy, organization, and technology. The FBI shares classified intelligence and other sensitive FBI data with federal, state, and local law enforcement officials through a variety of means, including the JTTFs, which partner FBI personnel with investigators from federal, state, and local agencies and are important force multipliers in the fight against terrorism. Since 9/11/01, the FBI has increased the number of JTTFs from 35 to 103 nationwide and has established the National Joint Terrorism Task Force (NJTTF) at FBIHQ, staffed by representatives from 38 federal, state, and local agencies. The NJTTF's mission is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of CT operations. The FBI agrees that effective information flow is critical and will continue to create new avenues of communication among law enforcement and intelligence agencies to better fight the terrorist threat.

The FBI's policy is to share by rule and withhold by exception. For example, while the FBI is committed to ensuring that its most sensitive law enforcement and intelligence sources and methods are protected from unauthorized disclosure, this is accomplished by sanitizing documents containing this information and then disseminating the resulting unclassified documents, rather than by merely withholding the unsanitized documents. The FBI has created a senior-level policy group, the Information Sharing Policy Group (ISPG), to ensure the framework

exists to facilitate compliance with the emphasis on broad dissemination. The ISPG is co-chaired by the FBI's EAD-I and EAD-Administration, and brings together the FBI entities that generate and disseminate law enforcement information and intelligence. Since its establishment in February 2004, this body has provided authoritative FBI policy guidance for internal and external information sharing initiatives. Working in conjunction with the Chief Information Officer (CIO) and his Program Management Executive (PME), the ISPG integrates information technology initiatives with FBI mission objectives, policy guidance, and legal authorities.

The FBI has also made technological and organizational changes to improve the flow of terrorism information between the FBI and state and local law enforcement agencies. Through our National Information Sharing Strategy (NISS), the FBI is implementing new technological tools to facilitate the sharing of regional and national criminal data with law enforcement agencies. NISS has three components: National Data Exchange (N-DEx), Regional Data Exchange (R-DEx), and Law Enforcement Online (LEO). N-DEx is the first national information sharing service. It will collect and process crime data from all major FBI databases, including the National Crime Information Center (NCIC), and will combine and correlate data to permit "one-stop shopping." N-DEx will give users access to information that will assist them in detecting and preventing terrorist attacks, in linking cases, and in forming broader investigative partnerships. Currently, N-DEx is in the pilot phase of operations, with full capability anticipated in 2007.

As a complement to N-DEx, R-DEx will enable the FBI to share data, including documents from its investigative files, electronically across federal, state, and local boundaries, improving the ability to prevent terrorism and other crimes by supplying the tools for using information in new analytical ways. R-DEx will also dramatically reduce the time spent by analysts in routine data entry, collation, and manual data manipulation by providing integrated information for use by all law enforcement agencies and by facilitating the analysis of law enforcement information, including queries, associations, and linkages to automated reports. The first R-DEx regional systems are in St. Louis and Seattle.

LEO, the third NISS component, uses Web-based communications capabilities to permit the law enforcement community to exchange information, conduct online education programs, and participate in professional special interest and topically focused dialog. LEO, which has been operational since 1995 and presently serves more than 42,000 users, has secure connectivity to the Regional Information Sharing Systems network. FBI intelligence products are disseminated weekly through LEO to more than 17,000 law enforcement agencies, providing

information about terrorism, criminal, and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public. Enhancements have permitted LEO to serve as the primary channel for Sensitive But Unclassified communications with other federal, state, and local agencies. The FBI also uses LEO to share intelligence products with Homeland Security Information Network (HSIN) users; states and major urban areas use the secure HSIN to obtain real-time interactive connectivity with the Homeland Security Operations Center and to share information with other HSIN users at the Sensitive But Unclassified level.

In addition to these technological enhancements, the FBI has also made organizational changes to enhance coordination with state and local law enforcement authorities. Among these was the establishment, in April 2002, of the Office of Law Enforcement Coordination (OLEC). Headed by a former state police chief, OLEC is responsible for ensuring that relevant intelligence is shared, as appropriate, with state and local law enforcement. As outlined in the FBI's Intelligence Policy Manual, the DI also shares information with our partners in state and local law enforcement through Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments.

In September 2003, the FBI also established FIGs in all Field Divisions. FIGs centrally manage the intelligence production and dissemination in FBI field offices, ensuring that state, local, and tribal law enforcement partners receive all relevant intelligence to support their missions. Among the key initiatives in this area is the joint development of intelligence requirements, along with state, local, and tribal partners, that clearly convey to FIGs the needs of those partners. In addition, in August 2005 the FBI worked with the Global Intelligence Working Group Requirements Subcommittee to develop a standing set of intelligence requirements for the United States Intelligence Community (USIC) and state, local, and tribal law enforcement with respect to national security and criminal intelligence topics. Once approved by the Criminal Intelligence Coordinating Council, this document will serve as the principal guidance for intelligence sharing between the FBI and other law enforcement organizations.

For information concerning the role of the Terrorist Screening Center (TSC) in sharing this important information, please see the response to Question 46.

7. In recent articles in the *New York Times* and other news sources, municipal police chiefs from New York, Los Angeles, Washington, D.C., Chicago, and Las Vegas repeatedly cite the FBI's unwillingness to share raw intelligence on a regular basis with their departments that would allow them to focus on the immediate threats in their cities. Washington Metropolitan Police Chief Ramsey stated, "I don't need a threat assessment. I need to know what I can do to proactively strengthen the security of our transit system." Is the FBI willing to allow local police departments' regular and immediate access to raw intelligence that is related to counterterrorism efforts in their jurisdictions?

Response:

As indicated in response to Question 6, above, the FBI has taken affirmative steps to improve the quantity and quality of shared raw intelligence, and we will continue to seek ways of improving that process.

8. Municipal police chiefs across the U.S. are discussing the formation of a nation-wide municipal counterterrorism network to supplement the flow of information from the FBI and DHS. Much of the discussion of this network has centered on the NYPD model of stationing agents in overseas countries to gather instant information that the FBI and DHS deliver hours or days later.

a. Does the FBI support this effort by local law enforcement to create its own national counterterrorism network?

Response:

The FBI considers state, local, and tribal law enforcement to be core nodes in the national CT network. We believe it is essential that such a network be part of the larger U.S. Information Sharing Environment (ISE), which is established under the direction of the ISE program manager pursuant to section 1016 of the IRTPA. Information sharing is crucial in the war on terrorism, and the FBI works with and participates in many of the regional fusion centers and other information sharing ventures that have already been established to ensure both that information from the national level is shared with state, local, and tribal law enforcement and that information developed by local law enforcement agencies is disseminated and shared with the national CT community, as well as with our foreign allies under appropriate circumstances.

The FBI defers to the Department of State for a judgment concerning the extent to which independent activities of state, local, and tribal law enforcement networks overseas may complicate U.S. foreign policy.

**b. Does the FBI view this movement towards a national municipal counterterrorism network as a failure in their intelligence dissemination network?**

Response:

The FBI does not view this initiative as a failure, but instead as a vital part of the nation's ISE.

**c. What plans does the FBI have to fix this perceived problem?**

Response:

The FBI's strategy to improve the flow of information through policy, organization, and technology is articulated in response to Question 6, above.

**9. The FBI's lack of promptly sharing important terrorist information is so well known, that CNN uses the fact that local police obtain information sooner from CNN than from the FBI or DHS as a marketing tool in a prime-time commercial quoting local law enforcement that they receive their first information on terrorist activity from CNN.**

**a. Provide any written internal memoranda referring to this commercial and any written or oral response made by any FBI personnel to CNN.**

Response:

We are aware of neither written internal memoranda referring to the commercial nor written response to CNN. We are also not aware of any oral discussions between the FBI and CNN regarding the commercial.

**b. Provide a copy of any written communication and a written summary of any oral communication with any local law enforcement agents concerning this commercial.**

Response:

Both oral and written communications with local law enforcement officials are frequent and wide ranging. While no such communications regarding the CNN commercial have come to the attention of senior FBI officials, we have no way of knowing whether informal communication on this topic has occurred.

10. The creation of the Information Sharing Environment ("ISE") has been described by some as marginalizing the responsibilities of the Department of Homeland Security by giving the information-sharing responsibilities of the federal government to a new agency.

a. How does FBI expect to interact with the ISE and what, if any, does FBI see as the role of the Department of Homeland Security in terrorist information sharing?

Response:

The FBI does not view the creation of the ISE as marginalizing the responsibility of any federal agency, including the Department of Homeland Security (DHS), and believes DHS's information-sharing role is defined in the Homeland Security Act of 2002. The ISE, specifically the ISE program manager, will establish information sharing technical standards and policies. The day-to-day sharing of content will occur in consonance with these standards, but will be accomplished by the individual agencies that comprise the U.S. CT network. The FBI expects to play a significant role in the ISE, including through the information sharing strategies discussed in response to Question 6, above, and will adjust its technical standards and policies to conform with those of the ISE.

Through the DI, the FBI has established FIGs in all field offices to ensure that terrorism intelligence needed by other agencies is extracted from investigative reports and disseminated to those agencies. This dissemination occurs at all levels of classification through direct message traffic and Web-based networks classified at the Top Secret-SCI level, the Secret level, the Sensitive But Unclassified level, and the Unclassified level. All FBI systems, networks, and communications channels will become part of the national ISE under the framework being developed by the ISE program manager, and the FBI is committed to using this framework to share as much terrorism information as possible. This commitment is reflected in the issuance of an Intelligence Policy Manual that provides specific guidance and emphasizes techniques to assist analysts in writing for dissemination.

The FBI does, however, remain committed to enforcing access controls to protect its most sensitive law enforcement and intelligence sources and methods from unauthorized disclosure in appropriate circumstances (such as when unauthorized disclosure would present a grave risk of compromise to the FBI's ability to obtain information about difficult collection targets). To maintain such protection, information may be disseminated in sanitized or declassified versions that are more easily used and shared by recipients.

**b. How many employees does FBI plan on providing to ISE as "detailees?"  
If any, when and who will FBI provide?**

**Response:**

The FBI is working with DOJ, the DNI, and the ISE program manager to determine the appropriate number of detailees, as well as their skill mix.

**c. What other resources does FBI expect to provide to ISE and when?**

**Response:**

Both DOJ and the FBI are prepared to offer any and all of our information technology and content to the ISE program manager, and are working with the program manager to ensure the appropriate integration of those resources into the ISE.

**11. The FBI has in the past three years spent over \$170 million dollars on the Virtual Case File system (VCF), only to recently inform the American people that all of their tax dollars were spent with nothing to show. Now the FBI has announced the all new Sentinel program as the system to fix all of their programs.**

**a. What specifically will happen that will ensure that Sentinel will not be another multi-million dollar fiasco?**

**Response:**

As the FBI advised during the hearing, we recognize that the development of Virtual Case File (VCF) suffered from inadequate managerial control and changing technical requirements. Using a disciplined programmatic approach in Sentinel's development will allow us to leverage the lessons learned from that effort.

Among other things, this programmatic approach has led to the development of a new Life Cycle Management Directive (LCMD), which specifies numerous criteria for passage through strict control gates. Each step of the process is approved by an appropriate Information Technology (IT) governing board, as outlined in the LCMD, before the program can progress to the next step. This process is discussed further in response to Question 11e, below. Several other key factors will also contribute to the success of the Sentinel program.

- The assignment of dedicated, experienced program oversight personnel.



- Early formation of processing teams comprised of both government and contractor representatives.
- Rigorous application of Earned Value Management System (EVMS) controls (discussed in response to Question 11e, below).
- Award of the contract to a "best value" contractor – one with dedicated, experienced personnel and a proven track record.
- A disciplined award-fee contract process.
- A rigorous "change control" process to reduce technical requirement revisions.

In addition, the following efforts should significantly improve the efficiency and effectiveness of the Sentinel development process.

- Commercial off-the-shelf software will be used whenever possible to decrease development and maintenance expenses, time, and risk.
- The use of a modular, loosely coupled architecture will allow the easy replacement of components. A failure of one component will not cause the whole system to fail, which will reduce overall program risk. If necessary, individual commercial products can be quickly and easily replaced with other comparable products with minimal impact on the whole system. This modular design will also facilitate component upgrades and replacements as newer versions evolve.
- The flexible architecture will allow for rapid re-configuration if the FBI's business needs change.
- The use of prototypes of key Sentinel components (workflow, portals, and security managers) will permit the identification of potential integration issues before they would be encountered through a fully deployed Sentinel program. The use of these prototypes will also allow early user feedback, reducing the risk that Sentinel will not meet users' needs. Permitting operational users access to the prototypes before Sentinel is fully developed and deployed will also provide early operational benefits.

**b. Provide copies of FBI Request for Proposals and any responses thereto regarding the Sentinel program.**

**Response:**

The Sentinel Statement of Work is attached (Enclosure A).

Responses to the RFP constitute "source selection information" as defined by 41 U.S.C. § 423(f)(2), release of which is generally prohibited by law (41 U.S.C. § 423(a)). Because the disclosure of this information would jeopardize the integrity of the procurement process, and because information from vendors is proprietary to them and not the Government's information, we decline to disclose those responses.

**c. What is the FBI budget for this new system?**

**Response:**

The FBI has developed a cost estimate to be used for budgetary purposes, but revealing it would alert potential contractors to the government's expectations regarding contract price, which would compromise the ability of the source selection process to identify the lowest responsive, responsible bidder. The FBI will have a final cost estimate when the contractor is selected.

**d. Provide the schedule of expected milestones in this project.**

**Response:**

The time frames in which milestones will be completed is a matter that will be addressed through the contract bid process, so the schedule will not be determined until the contract is awarded (in fact, the schedule will not be finalized until the completion of a review scheduled to occur 6 weeks into the first phase). While the schedule will continue to be notional at the time of contract award, we would be pleased to provide it to the Committee at that time.

The attached chart (Enclosure B) depicts four notional phases, including project reviews, control gates, and other controls associated with each phase.

Phase I establishes a single point of entry for legacy case management; expands the search capability to include IntelPlus file rooms; provides browser access to investigative data without requiring that browsers understand the changes in system architecture; and subsumes and expands current Web-based Automated.

Case Support (ACS) capabilities by summarizing a user's workload on a dashboard, rather than requiring the user to perform a series of queries to obtain it. To simplify data entry into the Universal Index (UNI), an entity extraction tool will be used to automatically index appropriate persons, places, and things. Finally, the core infrastructure components will be selected during this phase, and may include an Enterprise Service Bus and foundation services.

Phase II provides case document management and a records management repository, beginning the transition to paperless case records and implementing electronic records management. A workflow tool will support the flow of electronic case documents through their review and approval cycles, and a new security framework will support role-based access controls, single sign on, externally controlled interfaces, and electronic signatures based on Public Key Infrastructure. This phase addresses the concerns of the users of Sentinel's Initial Operating Capability that a paperless environment is necessary to leverage the benefits of automated workflow.

Phase III replaces and improves the Bureau-wide global index for persons, places, and things. In the "Connect the Dots" paradigm, the "dots" are represented by UNI, the legacy index that is, in effect, a database of entities (i.e., persons, places, and things) that have case relevance. Unlike the current UNI index, which supports a limited number of attributes, the new global index will improve the richness of the attributes associated with the indexed entities, permitting more precise searching.

Phase IV implements the new case and task management and reporting capabilities and will begin the systematic consolidation of case management systems.

e. Provide the system by which each stage of production of the program will be measured.

**Response:**

As indicated in response to Question 11d, above, the Sentinel program is employing a multi-tiered system of program management tools and practices to measure each stage of system development. Following are the three major program management tools and practices to be used by the Sentinel program.

1. Adherence to and expansion of the oversight process outlined in the FBI's IT LCMD. During each of the four phases of the Sentinel system's development, independent, senior executive boards will conduct six

separate control gate reviews. Each of these reviews must be favorable before Sentinel development can proceed. Each phase of the Sentinel system's development will also be the subject of 12 program-level reviews to measure that phase's progress. The standard FBI IT LCMD oversight and management process has been expanded for Sentinel by additionally requiring:

- An Acquisition Plan Review by the FBI Investment Management/Project Review Board before awarding contract options for Phases II, III, and IV.
  - An Integrated Baseline Review immediately following the award of the base contract and each contract option to ensure EVMS policies and procedures are in place and adequate.
  - A Delivery Acceptance Review near the end of each phase of Sentinel development to ensure that all work has been completed properly, including the training of field personnel and the accomplishment of organizational change management tasks.
2. Adherence to the use of EVMS principles and practices recommended by the Program Management Institute and Defense Acquisition University and mandated by the Office of Management and Budget. The Sentinel Program has embraced and mandated the use of EVMS principles and practices to measure the progress of each phase against an EVMS baseline (cost, schedule, and performance). The Sentinel Statement of Work requires that the provisions of FAR Case 2004-019 (published in the *Federal Register* on 4/8/05) be followed. Among other things, this requires the prime contractor to furnish a monthly progress report with respect to each phase's EVMS baseline and must provide the reasons for variances of more than five percent.
3. Use of an Independent Validation and Verification (IV&V) authority. Each phase of the Sentinel system's development will be independently measured and reported on by an IV&V authority. Throughout the development and deployment contract, this independent authority will measure progress and performance against the performance baseline. The results of these independent measurements will be reported to the FBI's CIO and PME.

12. The 9/11 Commission Staff Report no. 9 (pg. 9) faulted the FBI for having poorly trained and unqualified analysts.

a. Has the FBI changed its policy of hiring internally? Has there been any policy change that would allow for and that has resulted in the hiring of educated, trained and experienced analysts from external sources?

Response:

The 9/11 Commission's criticism of the qualifications of FBI analysts was based on an internal FBI document published in 1998 that asserted that two-thirds of FBI analysts were not qualified. The basis for the judgment expressed in that document is unclear and, in any event, is no longer accurate. In the 7 years since its publication, the FBI has established policies and systems to ensure the FBI's IAs are of the highest competence and quality. With the benefit of these new policies and systems, over the past two years we have hired more than 1,100 IA applicants possessing one or more critical skills. Of these recent hires, 59% had related intelligence or analytical experience, 47% had military experience, and 38% had advanced degrees.

A key component of this recent policy has been creation of the Intelligence Career Service (ICS), which demonstrates the importance of the FBI's intelligence mission and elevates the stature of its intelligence professionals. To develop the ICS, the FBI looked to both other elements of the USIC and the FBI's selection systems for best practices, creating a selection system implementation plan that would ensure selections based upon competencies identified for IAs, Language Analysts (LAs), and Physical Surveillance Specialists. (A "competency" is a cluster of related knowledge, skills, and abilities needed to perform a specific job.) These competencies correlate with job performance, can be measured against standards, and can be improved through training and development. Competency models allow for maximum reuse of human resources tools (such as testing and training courses) to assess and develop commonly required skills. Competency models also allow for the development of unique tools to assess and develop specialized skills. The competencies define our selection and hiring, training and development, performance management, Intelligence Officer Certification, retention, and career progression. They also help target and assess applicants, including those from within the FBI, with critical skills in intelligence, foreign languages, technology, area studies, and other specialties.

In furtherance of the effort to attract and retain IAs with critical skills, the FBI has also implemented three scholarship programs:

1. The Pat Roberts Intelligence Scholarship Program (PRISP) enhances the FBI's retention of IAs with specialized critical skills. Through the PRISP, the FBI can grant \$25,000 scholarships to current employees to help fund their past, current, or future studies in specialized skills or areas deemed critical by the FBI.
  2. The Cooperative Education Program offers to college juniors and seniors who are pursuing studies in critical Intelligence Program skills the opportunity to attend school full-time during part of the year and work at the FBI full-time during part of the year. Program participants receive FBI salaries and benefits, as well as tuition assistance.
  3. The Educational Attainment Internship provides financial assistance to selected high school seniors who will be pursuing college level work in a discipline deemed operationally critical to the FBI.
- b. How many analysts have been hired since 9/11 from external sources?
- c. How many analysts have been hired since 9/11 from internal sources?

Response to subparts b and c:

As indicated below, FBI records indicate that from FY 2002 through 8/18/05 the FBI has hired 377 IAs from within the FBI and 958 from outside the FBI (the number of external hires may include some FBI personnel who applied to external job postings). Regardless of the source of the candidate, all IA candidates are selected according to the same competency-based criteria, and successful IA candidates must meet these criteria.

<u>Fiscal Year</u>	<u>Internal Sources</u>	<u>External Sources</u>
2002	56	40
2003	77	173
2004	141	208
2005 (thru 8/18/05)	103	537

13. Since 9/11, the FBI continued to be plagued by a shortage of qualified analysts and translators. In the *New Yorker* article, the New York Police Department (NYPD) was able to resolve their analyst and translator problem by drawing upon immigrants who were intimately familiar with the languages and cultures under survey (pg. 64). These languages included Farsi, Arabic, Pashto, Dari and 60 other languages.

a. Has the FBI launched a similar program to address this issue?

b. If not, why not?

**Response to subparts a and b:**

For the last several years, the FBI has aggressively recruited from ethnically diverse communities throughout the United States to meet its translation requirements. In addition to traditional media campaigns, the FBI's National Recruiting Team and DI personnel have targeted specialty conferences, career fairs, university foreign language departments, and other forums to recruit those with critical language skills. FBI management officials also regularly host community meetings and speak at local events to generate interest in FBI employment and contractor opportunities. Beyond this, the FBI has partnered with organizations such as the U.S. Copts Association, Arab American Anti-Discrimination Committee, Arab American Institute, Network of Arab American Professionals, and Muslim Public Affairs Council to establish good will with their membership and to encourage those with critical language skills to consider FBI employment. Collectively, these efforts have resulted in more than 80,000 applications for linguist positions since 9/11/01 (most often, FBI linguists begin as contract linguists, so the majority of these applications have been for contract linguist positions that often evolve into FBI employment as LAs).

More than 3,000 FBI employees and contractors, including 397 LAs and 1,004 contract linguists, now have certified foreign language proficiency scores at or above the working proficiency level. More than 95% of the FBI's linguists are native speakers of a foreign language. These native-level fluencies and long-term immersions in foreign cultures ensure firm grasps of not only colloquial and idiomatic speech but also of heavily nuanced language containing religious, cultural, and historical references. Trustworthiness, as demonstrated through the security clearance process, is, of course, required of all FBI employees, including linguists.

14. This same article reports that the CIA and Pentagon have both asked the NYPD to assist them with translations, investigations and analysis of information relating to national security (pg. 64).

a. Has the FBI made use of the NYPD translation and analysis program?

b. If not, why not?

c. If so, set forth those instances in which the NYPD program has been used by FBI?

Response to subparts a, b, and c:

The FBI has not made use of the NYPD's translation and analysis program. In 2003, the FBI's Chief of Language Services met with the Deputy Commissioner of the NYPD to discuss common translation challenges and to explore the feasibility of sharing translation resources. During this meeting, the NYPD indicated that it did not want its officers and translation staff to undergo FBI polygraph examinations as a condition of their access to FBI information (the FBI requires that all candidates for its translator position submit to polygraph testing as a condition of being granted access to national security information). We understand that the CIA and Pentagon have found a means of ensuring trustworthiness without the use of polygraph examinations. We will work with both organizations to learn more about this process and will evaluate our ability to do the same.

15. The NYPD recruits immigrants from the Asia, Africa and the Pacific Islands to find qualified analysts and translators.

a. Does the FBI have a similar recruiting policy in place that targets immigrants?

b. If not, why not?

c. If so, provide statistics showing the results of this recruitment effort.

Response to subparts a, b, and c:

The FBI makes extensive use of LAs recruited from immigrant communities. We hire from those communities consistent with Executive Order (EO) 12968, "Access to Classified Information," which provides that "access to classified information shall be granted only to employees who are United States citizens".



(Section 3.1(b)). This EO substantially limits the FBI's ability to use the services of non-citizens, because nearly all of the FBI's CT and CI information in need of translation is classified at the "Secret" or "Top Secret" level. The EO does not, however, apply to state and local law enforcement agencies, who are free to establish their own standards for access to law enforcement information and may therefore obtain the assistance of immigrants without U.S. citizenship to meet translation requirements.

**16. On multiple occasions the FBI has been criticized for having thousands of hours of untranslated terror intercepts, including most recently in the OIG report dated July 27, 2005. One of the FBI's reasons for the backlog of untranslated intercepts is the lack of cleared analysts and translators.**

**a. Would the FBI agree to certify local or state law enforcement security checks for the purpose of clearing analysts and translators to assist the FBI?**

**b. If not, why not?**

**Response to subparts a and b:**

The FBI can authorize state or local law enforcement to conduct security checks of analysts and translators if those authorities conduct the checks in accordance with EO 12968. Generally, the requirements of EO 12968 are not met by state and local law enforcement agencies.

**c. Is it true as the OIG reports that it takes the FBI an average of 16 months to hire a contract linguist - an increase in time from prior years studied?**

**Response:**

An audit conducted by the DOJ Office of Inspector General (OIG) during 2003-2004 used the averages of the four applicant processing stages to determine a total cycle time of 14 months. A subsequent OIG audit adopted an entirely different methodology, including periods of time beyond the FBI's control, to determine that the total cycle time is, instead, 16 months. The difference between the 14-month and 16-month processing times is accounted for by these periods beyond the FBI's control, such as periods in which an applicant is out of the country and therefore unavailable for polygraph.

The FBI believes that the better measure of our processing efficiency is the 14-month applicant processing time. Under this methodology, a contract linguist candidate who successfully completes each stage of the employment process can

expect to remain in the process for 425 days before receiving the required "Top Secret" security clearance.

<b>Contract Linguist Applicant Cycle (FYs 2004-2005)</b>				
<b>Phase</b>	<b>Annual Volume</b>	<b>Pass Rate</b>	<b>Current Cycle Times (Median)</b>	<b>FY 07 Target (Approximate)</b>
Professional Testing	3,000	25%	158 days	60 days
Polygraph	600	58%	65 days	30 days
Background Investigation	350	85%	95 days	60 days
Security Adjudication	300	90%	107 days	30 days
<b>Total</b>	<b>270</b>	<b>13%</b>	<b>425 days</b>	<b>180 days</b>

All contract linguist candidates are subject to a thorough pre-contract vetting process that is both labor and time intensive. Contract linguist candidates must pass proficiency tests in both English and a foreign language. In addition, because they must be granted "Top Secret" security clearances, each candidate's pre-contract vetting process includes the following:

- Personnel security interview conducted by appropriately trained FBI SA or security personnel.
- Polygraph examination focused on the candidate's involvement in foreign counterintelligence matters, purpose in seeking FBI employment, application accuracy and thoroughness, and prior involvement in the sale or use of illegal drugs.
- Single-scope background investigation covering the most recent 10-year period of the candidate's life or longer.
- Risk analysis of the background investigation package conducted by FBI CI and/or CT subject matter experts.

**d. If true, how can FBI hire qualified, highly marketable, people when they must wait over a year to find out if they are going to be hired?**

**Response:**

The FBI shares your concern. We are working to reduce the time required for the applicant vetting process from 425 days to approximately 180 days by FY 2007 through the implementation of process improvements recommended by a business process reengineering firm and the National Academy of Public Administration. Among other means to this goal, the FBI plans reduce the proficiency test cycle from 158 to 60 days by the end of FY 2006 by automating its language proficiency test instruments and using third party test centers. The FBI also anticipates reducing the background investigation and security adjudication cycles from approximately 200 days to 90 days by FY 2007 by consolidating background investigation functions within the Security Division and reorganizing to streamline associated activities.

**e. If true, do the inevitable changes in the terrorist landscape and therefore the particular languages in need of translation, require an expedited hiring process in order to keep up with the ever changing war on terrorism?**

**Response:**

The FBI can and often does respond to operational exigencies through the expedited processing of contract linguist candidates. For example, in 2005 several contract linguist candidates with proficiency in an urgently needed African language were recruited and fully vetted through proficiency testing, polygraph, and background investigation in 30 days or less. This rapid response capability, while extremely manpower intensive, ensures the FBI can quickly respond to the most critical national security requirements.

The FBI recognizes that with the ever-changing face and voice of global terrorism, we must be prepared to respond to translation requirements associated with the world's most obscure languages. Geopolitical indicators and threat forecasts provide a foundation for the FBI's translation planning.

f. If untrue, how long does it take FBI, on average to hire contract linguists and is this time reasonable?

Response:

Please see our response to Question 16c, above.

17. The FBI translation program has been criticized for having excessive and unreasonably high standards when it comes to pre employment language testing. There have been newspaper articles detailing that, for instance, University Professors who teach Arabic were unable to pass the test.

a. Is the FBI testing standard [ ] too high?

b. What, if any, changes are planned in this testing process to avoid these unreasonably high testing standards?

Response to subparts a and b:

The FBI evaluates language tests in accordance with Interagency Language Roundtable (ILR) Skill Level Descriptions, approved by the Office of Personnel Management as the standards for government-wide use in 1985, and uses the Defense Language Proficiency Test, prepared by the Defense Language Institute, to test foreign language listening and reading skills. The ILR employs a scale of 0 to 5, describing Level 2 as "Limited Working Proficiency" and Level 3 as "General Professional Proficiency."

The passing score for FBI verbatim translation exams is 2+ or 3, depending on the score received in the speaking proficiency test. When applicants with knowledge of a foreign language fail a translation test it is typically because good translation requires not only proficiency in two languages but also what the ILR describes as "congruity judgment," or the ability to choose the best accurate equivalent from among possible translations.

**18. With the recent terrorist attacks in London, intelligence analysts are saying, and the American public is concerned, that an attack on American soil is imminent.**

**a. How is the intelligence community – FBI, ISE, DOJ – preparing to protect us against such an attack?**

**Response:**

In response to the London mass transit attacks, the FBI has been assisting British authorities in their investigation and has been investigating any and all connections to the U.S. to prevent a similar attack here. One phase of this effort has been the production of an unclassified daily Intelligence Bulletin that communicates current investigative updates and other information that might be useful to state and local law enforcement authorities. Among other things, these bulletins have articulated the tactics and techniques used in the London bombings and detailed the chemical composition of the explosives used in the attacks. These bulletins have been provided to all FBI field offices and to our law enforcement partners.

**b. What has the FBI learned from the London attacks that can help prevent a mass transit attack in the U.S.?**

**Response:**

The FBI continues to investigate the London bombers' relationships and contacts, including their financial and communications links, to identify any persons who might pose a danger to the U.S. We remain concerned that the London attacks could serve as a template for an attack in the U.S. in which a few "home grown" extremists might target a metropolitan subway system using relatively small quantities of homemade explosives. The FBI is more committed than ever to working collaboratively with state and local law enforcement, who are often the most effective first line of defense in identifying and disrupting attacks.

**19. In testimony before the Senate Committee on Foreign Relations in 2002, President Henry Kelly of the Federation of American Scientists reported that "significant quantities of radioactive material have been lost or stolen from US facilities in the past few years." He also stated that much of this material is useful for the construction of radiological dispersion devices and dirty bombs.**

**a. What is the FBI doing to track and recover lost or stolen radiological material in the U.S.?**

**Response:**

The FBI maintains a close relationship with the agencies involved in licensing the possession of nuclear/radiological material (including the Department of Defense (DoD), Department of Energy (DoE), and Nuclear Regulatory Commission (NRC)). Pursuant to the FBI's Nuclear Site Security Program, we have directed our field offices to establish close liaison with appropriate security personnel at nuclear sites in order to ensure prompt notification and response to suspicious activity, including attempts to illegally obtain nuclear or radiological material. We have also reiterated to all field offices the need for aggressive investigation of lost, stolen, or missing radioactive source material and the importance of ensuring that state and local law enforcement authorities promptly notify the FBI of such incidents. Coordination of these issues has been greatly facilitated by the development and enhancement of the JTTF program because the JTTFs, which are comprised of federal, state, and local law enforcement representatives, are invaluable assets in the sharing of information and coordination among law enforcement agencies. The FBI also participates in a number of interagency working groups at the Headquarters level in order to develop U.S. Government policy options for preparing for, preventing, responding to, and recovering from a radiological attack. These working groups have undertaken numerous tasks, including the review of existing security and licensing regulations for adequacy and appropriateness and the development of a National Source Tracking System to better account for individual radiological sources in the possession of NRC licensees, which include medical, industrial, and academic entities.

**b. Provide a list of all known lost or stolen radiological material in the U.S.**

**Response:**

The NRC-managed Nuclear Materials Event Database indicates that since January 2003 NRC licensees reported approximately 1,300 events involving lost, stolen, or abandoned radiological sources. The NRC estimates that approximately 50 percent of these radiological sources are eventually recovered.

While statistics such as these may appear to indicate a significant loss of material, the majority of these incidents involve minute quantities of radioactive material present in industrial equipment used in radiography and well logging. Such equipment often contains "low hazard" material with a short half-life. While the FBI is concerned with all reports of lost, missing, or stolen nuclear or radiological material, and coordinates closely with the cognizant agencies in aggressively investigating these allegations, the vast majority of these incidents appear to be inadvertent rather than the product of criminal intent, do not pose a harm to public safety, and are therefore not considered "significant" for CT purposes.

**20. There are currently seven sites in the U.S. that handle Category I special nuclear material, or nuclear material that is considered weapons-grade material.**

**a. What role does the FBI have in securing this material from theft?**

**Response:**

The FBI is responsible for investigating allegations of unlawful use or possession of nuclear or radiological materials, and threats to use such materials, for terrorist or other criminal purposes. This responsibility includes all man-made radiological materials (those used in reactor operations as opposed to those that occur naturally), which may run the gamut from weapons-grade materials (Category I Special Nuclear Material (SNM)) to radiological source materials. Such misuse may be prosecuted through a variety of statutes.

DoE's National Nuclear Security Administration (DoE/NNSA) bears primary responsibility for the safety and security of its nuclear facilities, including those that handle Category I SNM. As part of its overall Nuclear Site Security Program, the FBI coordinates closely with these sites in a proactive effort to prevent terrorist or other criminal activities directed against these sites. Such efforts include both routine liaison activities (such as intelligence sharing and threat briefings) and more specialized initiatives (such as joint training and exercises that typically focus on the coordination of emergency responses to potentially disruptive incidents).

**b. Is there a policy of standardized security procedures that must be followed by such facilities?**

**Response:**

DoE/NNSA adheres to an extremely rigorous and robust protection strategy based on the sensitive nature of the assets under its purview. This protection strategy is "graded" according to the type of material handled at a given site, with Category I SNM sites afforded the highest level of protection. Further information on this subject may best be obtained from DoE.

**c. If so, provide the standard security procedures and how these procedures are monitored by FBI.**

**d. If not, are there any written plans to do so? Provide written plans.**

**Response to subparts c and d:**

Security countermeasures are part of each site's protection strategy. The FBI is not responsible for monitoring DoE's protection strategy per se, but we do maintain a level of interaction with DoE through regularly recurring liaison and training, and this interaction facilitates a regular review of these procedures.

**21. In recent years, there have been a number of reported incidences of theft of documents and materials from Los Alamos National Nuclear Laboratory and other locations.**

**a. How does the FBI plan to reduce the number of thefts from these facilities?**

**Response:**

Pursuant to 50 U.S.C. § 402a, the FBI is to be "advised immediately of any information, regardless of origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power." The FBI has initiated proactive measures in order to better protect against the compromise of classified information, specifically addressing compromises in the national laboratories. The cornerstone of these measures is the Agents in the Lab Initiative.

Pursuant to this initiative, FBI SAs are embedded in the Internal Security Office of the Los Alamos National Laboratory (LANL). These SAs possess academic



credentials in mechanical and nuclear engineering, which lend themselves to the LANL's overall scientific and research mission. The LANL's Internal Security Office is responsible for the Lab's counterintelligence (CI) and counterterrorism (CT) activities, including: the conduct of CI briefings/debriefings for LANL personnel; response to internal CI inquiries regarding LANL employees, contractors, and visitors; and the identification of potential CI and CT risks and exposures to Foreign Intelligence Services and terrorist organizations. The FBI has also assigned an experienced Santa Fe Supervisory Senior Resident Agent (SSRA) to focus on day-to-day LANL operations, permitting emphasis on espionage prevention and detection and strong partnerships with DoE and the CIA.

When FBI SAs investigate matters at the LANL, they share the resulting reports with DoE entities, including the LANL. DoE/NNSA uses these reports to develop "lessons learned" reports, identifying potential weaknesses in the internal security apparatus and providing recommendations to resolve concerns. In addition, the FBI's Albuquerque Division SAC meets regularly with the LANL Director to discuss all matters of interest. That meeting is attended by the Santa Fe SSRA and the LANL's Senior CI Official (who heads the Internal Security Office); the Santa Fe SSRA and LANL's Senior CI Official also meet separately each month to ensure maximum information sharing.

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

**b. Has FBI investigated these incidences?**

**Response:**

The FBI thoroughly investigates all reports of possible theft or compromise of classified documents or materials. Previous cases have been successfully resolved and future incidents are much less likely due to the implementation of more effective and efficient administrative and security practices.

**c. How many such incidences remain unsolved? Provide date, time, location and circumstances regarding such unsolved incidences.**

**Response:**

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

**22. The NYPD currently treats all tractor-trailer and hazmat incidences as potential crime scenes, due to intelligence received about al Qaeda operating procedures.**

**a. Does the FBI have clearly defined procedures in place to facilitate cooperation between the FBI and local and state law enforcement officials to determine if an incident is an accident or a terrorist attack?**

**Response:**

The FBI's responses to all threats and incidents involving potential weapons of mass destruction (WMD) or other terrorist acts include assessments of credibility and interagency coordination. Typically, FBIHQ is notified of a suspected WMD threat or incident by the FBI field office in the location of the threat or incident. Upon such notification, or when FBIHQ otherwise becomes aware of such threats or incidents, FBIHQ's WMD Operations Unit (WMDOU) provides rapid assistance to the field, including execution of the following standard operating procedures:

1. Evaluation of the initial threat assessment (that initial threat assessment is often conducted by the FBI field office).
2. Completion of a comprehensive threat assessment.
3. Coordination of FBIHQ assets for response and the provision of technical support.

WMDOU, which is responsible for developing appropriate FBI response policy for such incidents, overseeing strategic threat assessments, and coordinating assets to assist FBI field divisions in their responses to domestic WMD threats or incidents, uses the threat assessment process to identify the resources needed for response. WMDOU calls on previously identified subject matter experts in other agencies and consults with FBI scientists and the FBI's Hazardous Materials Response Unit as appropriate to the incident. These technical experts are able to respond to chemical, biological, and radiological/nuclear incidents, as well as incidents involving explosive devices. In addition, FBI field offices have designated WMD Coordinators, who are responsible for developing strong relationships with federal, state, and local crisis and consequence management agencies. WMD Coordinators also maintain liaison with a wide range of emergency responders through the JTTFs (each of which includes representatives from state and local government) and participate in operational crisis response training and exercises with state and local counterparts. During a potential terrorist incident, the FBI would notify JTTF members so the response may be coordinated appropriately with law enforcement partners at all levels.

b. If so, provide a copy of those procedures and a description of all incidences in which the procedures have been implemented.

Response:

Both FBIHQ's WMDOU and FBI field offices respond to large volumes of threats, rendering it impracticable to provide an exhaustive list describing these incidents.

Homeland Security Presidential Directive 5 required the development of a National Response Plan (NRP) to align Federal coordination structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic incident management. The 426-page NRP, which is available in full on DHS's website, provides the protocols for response to domestic incidents, including nuclear and radiological incidents, biological incidents, and other acts of terrorism. While much of the NRP concerns response to incidents such as the tractor/trailer and hazardous materials incidents on which this question focuses, the most relevant portions of the NRP are the Terrorism Incident Law Enforcement and Investigation Annex, the Nuclear/Radiological Incident Annex, and the Biological Incident Annex. Those three annexes are attached (Enclosure C).

Questions Posed by Senator Leahy

23. In follow up questions to a June 6, 2002, hearing, you stated that agents at headquarters should have expertise in areas to which they are assigned. This would certainly include counterterrorism officials. You also said that field supervisors should have "extensive counterterrorism experience." Recently, we learned from depositions in a civil suit that the highest level of counterterrorism officials at the Bureau do not have specific prior experience in this area, nor do they think it is important for them to possess such expertise.

a. How can we reform the FBI if it insists that traditional law enforcement experience is *all* that is needed to prevent and prosecute acts of terrorism?

Response:

We respectfully disagree with the assertion the FBI "insists that traditional law enforcement experience is *all* that is needed" to prevent terrorism. SA candidates for positions in all programs are required to demonstrate levels of experience and performance appropriate to the position, and increasingly rigorous standards are applied to progressively higher leadership levels.

Candidates for all SA mid-level management positions (generally, those at the GS-14 and GS-15 levels) are vetted through selection boards comprised of Senior Executive Service (SES) members representing priority divisions at FBIHQ, including CTD, CD, DI, CyD, and CID. For example, ASAC candidates (ASAC is a GS-15 position) are required to demonstrate competence in the following areas through the submission of two examples with respect to each area: communication, flexibility/adaptability, initiative, interpersonal ability, leadership, liaison, organizing and planning, and problem solving/judgment. Often, these examples identify the impact of the candidate's efforts on the FBI's highest priority matters, including CT accomplishments. Mid-level SA managers seeking promotion to entry level SES positions are required to submit résumés demonstrating success in five competencies: management, leadership, liaison, problem solving, and interpersonal ability. Within these competencies, candidates must show the highest levels of achievement in the FBI's top priorities. To the extent possible, these résumés also reflect successes in program areas applicable to the position being sought.

Throughout these multi-tiered vetting processes, strong managerial skills are considered critical, and subject matter expertise is considered and preferred, but is not mandatory. Typically, SAs who attain higher-level executive positions have first held other senior management positions in the FBI, such as SAC of a field

office, and through them have acquired management experience across both national security and criminal programs.

**b. Do you think that law enforcement experience is sufficient? Or do you believe that expertise in counterterrorism should be a prerequisite for counterterrorism leaders of the Bureau?**

**Response:**

After the events of 09/11/01, the FBI's top priority became the prevention of additional terrorist attacks against this nation. As part of this mission shift, we initiated the development of career paths for SAs that will require them to specialize in one of five areas: CT, CI, intelligence, cyber, or criminal. As this policy is implemented, the FBI will develop a cadre of SAs with subject matter expertise in each of these priority programs. Once this cadre is established, it may be appropriate for the FBI to consider mandatory subject matter expertise in certain positions. In the meantime, we believe it is appropriate to consider subject matter expertise as a factor, but not a prerequisite, when determining assignments.

Among the FBI's efforts to foster growth in these priority areas is a rotational program pursuant to which SAs are assigned to FBIHQ on a temporary duty (TDY) basis to address priority program needs. This program allows "field" Agents to bring "real world" experience to FBIHQ and to learn more about the "big picture" than is possible when working isolated cases. In FY 2004 alone, approximately 2,200 SAs benefitted from these TDY assignments.

**24. A panelist participating in the 9/11 Commission's Public Discourse Project reported that the Bureau has 200 unfilled counterterrorism positions and is facing difficulty finding analysts and agents to fill those posts.**

**a. How many counterterrorism positions at the Bureau are presently unfilled? What are the obstacles to filling these positions?**

**Response:**

As of 05/13/2005, there were approximately 202 vacant SA CT positions at FBIHQ. The primary obstacles to filling these positions, and positions at FBIHQ in general, are the recent spike in D.C.-area housing costs and the overall high cost of living in the Washington, D.C., area.

The FBI's success in recruiting analysts has been better. The FBI's FY 2005 goal was to hire 880 analysts. As of 8/29/05, we had hired 660 new analysts (including both external hires and applications from qualified FBI employees serving in other positions). An additional 376 applicants have been selected and are being processed for employment, and 72 analyst candidates have been approved for employment but are not yet on board. During the same time period, 103 analysts have vacated analyst positions through reassignment, transfer to other federal agencies, resignation, or retirement. These numbers indicate that there are no particular obstacles to filling analyst positions, but there is some difficulty in keeping analysts on board.

**b. What steps has the Bureau taken to fill these positions more rapidly?**

**Response:**

To ensure a constant flow of applicants for all critical positions, the FBI attempts to publicize the rewards of FBI careers through various means, such as national advertising strategies targeting applicants with critical skills, including minorities, women, and persons with disabilities. These strategies include interactive campaigns and targeted advertisements in magazines, journals, television, radio, billboards, airports, newspapers, and theaters. The advertisements feature onboard employees who have critical experience and education that matches the FBI's targeted hiring objectives. This year's special effort to attract applicants to the analyst positions included a television ad that aired during the 2005 Super Bowl.

In addition, partnerships and networking vehicles have been developed to expand awareness of the FBI's career opportunities within the African-American, Asian-American, Hispanic, Native American, and Middle Eastern communities, and by addressing women's organizations and physically challenged audiences. The FBI has also developed partnerships with faith-based organizations to improve awareness of the FBI in those communities, and has implemented numerous internship programs in order to enhance the FBI's visibility and recruitment efforts at colleges and universities throughout the United States.

In addition to attracting and retaining critical employees through the increased use of the student loan repayment program and relocation and retention bonuses, the FBI has developed an FBIHQ Term Temporary Duty Pilot Program, pursuant to which SAs may apply for designated 18-month term FBIHQ assignments during a 90-day window. Selectees will receive FBIHQ supervisory credit and will be authorized to apply for field desks as SSAs after 15 months. As of 08/30/2005,

this pilot project had generated 567 applications for positions at FBIHQ and is expected to greatly reduce the staffing shortfall.

Similarly, a combination of methods is being employed to fill analyst positions quickly and to keep them filled. Recruitment bonuses totaling approximately \$3.4 million were paid to approximately 380 analysts and retention allowances were afforded to two analysts in approximately the first 10 months of FY 2005 (many analysts are fairly new to the FBI and are not yet eligible for retention incentives). The availability of these bonuses is beneficial both because they encourage applicants to apply for analyst positions and because they encourage them to stay to complete the service to which they agree as part of the bonus offer. Retention has also been improved by our ability to increase access to the student loan repayment program, which also includes a service commitment. Whereas the availability of funds limited participation to 31 analysts during FY 2005, approximately 180 analysts participated in the student loan repayment program during FY 2005.

**25. In July, John Perry, chief executive of CardSystems, testified before the House Financial Services Subcommittee on Oversight and Investigations about a security breach that exposed as many as 40 million credit-card holders to potential fraud. Mr. Perry testified that CardSystems contacted the FBI about the data breach on May 23, but that the FBI took two days to respond, in part due to lack of clarity on the scope of the breach.**

**What is the FBI's policy on responding to reports of personal data security breaches, including how quickly agents should respond to such reports, and what expertise and forensic capabilities are available within the FBI to assess the scope of electronic data breaches?**

**Response:**

With respect to the CardSystems Solutions, Inc. (CSSI) breach, we would like to note that the FBI initiated investigation on the day it was contacted based on information provided by the CSSI General Counsel to the FBI's Phoenix Division. At that point, CSSI had already determined that the intruder had been active within CSSI's network for nine months and CSSI had implemented defensive measures to mitigate further compromise. These measures included attempts to determine the type of data compromised and the extent of the breach, during which CSSI used the file transfer protocol to improperly retrieve from the intruder's computer the files that contained crucial transaction data and corresponding security codes obtained by the intruder through unauthorized queries. It was after this discovery that the FBI was notified, 8 days after CSSI noticed the unauthorized activity and 4 months after CSSI was alerted by the card

associations that they believed other unusual activity could be traced to a possible compromise of CSSI data.

As with all information of possible criminal activity received by the FBI, information relating to possible computer intrusions is initially evaluated to determine the appropriate course of action. The FBI's response depends on the circumstances involved: is there a possibility of loss of life, terrorist attack, state-sponsored intrusion placing the national information infrastructure at risk, prevention of criminal activity or further financial loss? (In the CSSI case, the FBI was advised that CSSI had implemented defensive measures to mitigate further compromise.)

The FBI's CyD includes the Special Technologies and Applications Section (STAS), which is often called upon by other FBI Divisions, USIC agencies, state and local governments, and foreign partners to determine the "who, what, why, when, where, and how" of computer intrusions. Through written reports, electronic disseminations, and other means, the STAS helps IAs, investigators, and decision makers understand what level of sophistication the activity represents, where evidence of the intrusion may be located, and, in some cases most importantly, what data was viewed, modified, added, deleted, or taken, and where it might reside thereafter. STAS is commonly called upon to re-live the electronic "day in the life of a computer file" to explain who saw it, "touched" it, moved it, and so on.

**26. A June 2005 report by the Office of Inspector General evaluated DOJ's counterterrorism task forces and advisory counsels, including 3 led by the FBI: the Joint Terrorism Task Forces (JTTFs), the National Joint Terrorism Task Force (NJTTF) and the Foreign Terrorist Tracking Task Force (FTTF).**

**a. The report found management and resources problems, including frequent turnover in leadership of the JTTFs, lack of counterterrorism expertise within the task force membership, as well as insufficient training, standards or orientation for members. What specific actions will the FBI undertake to address these concerns?**

**Response:**

The FBI concurs with the findings of the DOJ Office of the Inspector General (OIG) regarding the importance of ensuring long-term, stable JTTF and Foreign Terrorist Tracking Task Force (FTTF) leadership, effective and available training in critical substantive areas, and, in the case of the FTTF, a settled location.



All FBI investigators, in all programs, view the quality and completion of investigations as a priority. JTTF participants currently receive training in basic core functions, and training has been developed and delivered (in various formats) regarding the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, basic security issues (including the proper classification of intelligence communications), the roles, missions, and operations of the USIC, the FBI's ACS system, the Investigative Data Warehouse (IDW), the Threat Reporting System, and the tools, techniques, and skills needed to successfully investigate terrorism.

A recently created CTD Unit has been charged with assessing CT training and professional development needs, including those of the JTTFs. This Unit is developing a comprehensive NJTTF/JTTF Training Manual that will include the topics listed below. These topics will also be addressed in training provided to newly appointed JTTF members within their first year of service.

- Administration
- Security
- Automation/Computer Investigative Resources
- Introduction to Foreign Intelligence/Terrorism
- International/Domestic Terrorism Basic Courses (CD-ROM based training)
- Foreign CI Basic Course (CD-ROM based training)
- Surveillance Techniques
- Evidence Procedures
- Technical Writing
- Legal Training
- Asset/Source Recruitment and Management

The FTTTF has faced numerous challenges since its creation, and the pursuit of some of its own initiatives have been delayed while it provided critical support to the early efforts of the TSC, which was also recently created. The FTTTF has addressed the early problems created by fluid leadership and organizational structure, and has recently been relocated to "permanent" space, which will further improve stability. The FBI concurs with the OIG's recommendation that the FTTTF develop and implement a marketing plan to improve awareness and understanding of its services, and has taken steps to implement such a plan. The FTTTF's efforts to increase awareness of its role and responsibilities have included weekly briefings to visiting SACs and ASACs, participation in CTD's orientation program for new assignees, presentations to the NJTTF Conference, briefings to new SACs and Legal Attachés, and briefings to outside organizations (including the International Association of Chief of Police, National Sheriffs'

Association, Major City Chiefs, Interagency Intelligence Committee on Terrorism, and Homeland Security and Information Sharing Conference). In addition, the FTTTF has established a site on the FBI's Intranet, which will be replicated in part on the Secret Internet Protocol Router Network, and has published an Executive Guide to provide a concise synopsis of FTTTF capabilities and the means of requesting support.

**b. In addition, the OIG report noted that the FBI has not signed Memorandums of Understanding (MOU) to define the roles, responsibilities, information sharing protocols and length of commitment with the agencies participating in these taskforces. When will the FBI have in place an MOU defining these critical elements?**

**Response:**

Since 1980, the FBI has maintained Memoranda of Understanding (MOUs) with the state and local agencies that participate in the JTTFs. The FBI currently has in place 311 MOUs with agencies participating in the NJTTF and JTTFs, updated since 9/11/01 to incorporate such issues as polygraph requirements, information sharing policy, and length of commitment by individual participants. The FBI's CTD is currently working with DoD and DHS to standardize these MOUs and anticipates that the existing MOUs will be updated in the near future.

**27. A recent report by the National Academy of Public Administration found that the FBI's information sharing practices are largely ad hoc with no mechanisms, such as penalties or incentives, to enforce or promote information sharing.**

**a. What progress has the FBI made in creating incentives to improve information sharing and penalties for failure to advance those goals?**

**b. What future actions does the FBI plan to improve its information sharing capabilities further?**

**Response to subparts a and b:**

Please see our response to Question 6, above.

28. In May of this year, it was reported that a search of IAFIS failed to identify the fingerprints of an individual detained by local authorities, Jeremy Jones, who was subsequently released and went on to kill three women and one teenage girl in three states. In addition, Mr. Jones is a person of interest in several other cases. An FBI official described the mistake as a "result of a technical database error, not a human examiner failing to make an appropriate match." What steps has the FBI taken to correct this database error and prevent a repeat of this type of mistake in the future?

Response:

The cause of the missed identification was a filter in the Automated Fingerprint Identification System (AFIS) component of the Integrated Automated Fingerprint Identification System (IAFIS). This filter, which was employed to narrow the field of records searched, erroneously eliminated Jones' record as a candidate because it was slightly outside the filter's parameters. When the FBI discovered this problem, it reviewed the need for the filter. Because of AFIS hardware upgrades completed in June 2004, it was determined that the filter was no longer necessary and should be disabled. This was accomplished on 1/9/05.

In addition to disabling the problematic filter, the FBI has taken several steps to ensure IAFIS' integrity. These steps have included an inspection of the system and the events that led to the missed identification, a search of the database to identify duplicate criminal history records, and the initiation of an aggressive program to detect and prevent missed IAFIS identifications. This program includes a quality assurance review of approximately ten percent of all transactions. In addition, because Jones used the exact name, date of birth, and social security number of another subject who was in prison at the time, causing additional confusion in making the identification, the FBI has initiated a review of all records that have exact matches of descriptive information to ensure they are not duplicate records and to provide investigative leads to law enforcement. Finally, the FBI has received funding for a 2006 effort to implement an overall enhancement of IAFIS that will involve substantial upgrades to the AFIS component. This broad enhancement was first conceptualized by the FBI, along with its law enforcement partners, in September 2003.

29. The consolidated watchlist uses 4 risk-based handling codes to designate how law enforcement should respond when encountering individuals on the list. A recent Inspector General report found that nearly 32,000 "armed and dangerous" individuals are designated for the lowest handling code. This code does not require law enforcement encountering those individuals to contact the TSC or any other law enforcement agency. Some of these individuals were also described as "having engaged in terrorism," "likely to engage in terrorism if they enter the United States," "hijacker," "hostage taker," and "user of explosive or firearms." In press reports, the FBI has countered that legal restrictions prevent officers from ordering a suspect held without an arrest warrant or other evidence.

Notwithstanding strategic reasons or legal requirements that weigh against immediate detention of these individuals, there is a legitimate concern about designating such individuals for the lowest handling. You indicated at the July 27 hearing that you would look into the matter and respond.

a. Why are individuals described in such dangerous terms designated for the lowest handling?

b. Is there a code that would allow TSC to designate these individuals in such a way that law enforcement encountering them would be aware of the possible danger or use the opportunity to update TSC on any encounters with those individuals?

Response to subparts a and b:

Director Mueller provided this information to Senator Leahy by letter dated 8/1/05. A copy of that letter is attached as Enclosure D.

It is important to understand that Handling Codes (HCs) are not associated with threat levels; all terrorism-related entries in the Violent Gang and Terrorist Offender File (VGTOF) are assigned HCs, and the first line on the NCIC screen for all these entries advises: "Warning, approach with caution." The purpose of assigning the different HCs is to identify the government's authority to take legal action with respect to the individual based solely on the individual's inclusion in VGTOF. Encounters with some of the 9/11/01 hijackers shortly before those attacks taught us the importance of arresting, detaining, or otherwise appropriately responding when those who pose a terrorist threat are encountered. If a local law enforcement officer encounters an individual for whom there is a pending arrest warrant related to terrorism (HC1), the officer needs to know to effect an immediate arrest. Similarly, a law enforcement officer who encounters an individual of investigative interest with respect to terrorist activity (HC2) needs to know to detain that person to obtain more information. Clearly, these individuals may be equally dangerous, so the HC doesn't identify the degree of danger they

pose to the law enforcement officer (in fact, the HC1 may be based on a warrant related to "white collar" terrorism financing, while the HC2 may be based on facts indicating bomb construction, so an HC2 could, in fact, be more dangerous to the officer than an HC1). Instead, the HC indicates what response by law enforcement is lawful and appropriate (arrest, detention, or otherwise) based on the information available to the TSC. All HCs request TSC notification so the TSC can assist in coordinating the response, and all HCs are subject to revision based on new information or changes in status.

HCs, which identify the permissible response if an individual is encountered, are unrelated to Immigration and Nationality Act (INA) codes, which are assigned by DHS to identify the nature of the derogatory information on an individual. We defer to DHS with respect to the assignment and use of INA codes.

**30. The OIG Report found that there is "no formal strategic plan" to guide the [Terrorist Screening] Center's progress, staffing, structure and future planning, but that such a plan would assist the TSC in addressing the most significant weaknesses identified in the OIG report. In addition, the Report noted that TSC has no formal procedure for evaluating its own performance. When will the TSC develop a formal strategic plan or procedures for performance evaluation?**

**Response:**

The TSC's formal strategic plan, dated 6/17/05, addresses the organization, structure, and progress of the TSC, including new initiatives, plan implementation, and progress reviews. The TSC's performance will be evaluated according to metrics designed to assess the quality of TSC data and its contribution to the performance and effectiveness of TSC customers. TSC will develop a means of using metrics to evaluate TSC performance over time, and each review will be assigned an owner, priority, start date, and projected end date.

31. In May 2005, the Government Accountability Office issued a report on U.S. passport fraud detection efforts and identified several weaknesses in those efforts, including that TSC neither provides consolidated terrorist watch list information to the State Department in a systematic manner nor routinely provides the names of other individuals wanted by federal and state law enforcement authorities. The Report indicated that the State Department sent a proposal on sharing watchlist information to TSC in January of 2005 and a written request outlining its needs for access to information on wanted persons in April 2005.

a. What steps has TSC taken to share with the State Department information from the consolidated watchlist and the FBI's database on wanted persons?

Response:

An MOU between the Department of State (DOS) and the TSC regarding the export of TSC data into the Passport Class System was signed by Assistant Secretary of State for Consular Affairs Maura Harty and by TSC Director Donna Bucella in late June 2005. The program was implemented on 7/25/05.

The FBI's database on "wanted persons" is managed by the FBI's CJIS Division, rather than by the TSC. In June 2005, the FBI began providing to DOS all NCIC "wanted persons" information derived from FBI files in order to enhance passport screening and fugitive apprehension. The FBI and DOS are in the process of completing an MOU to document this process. In addition, the FBI and DOS are attempting to coordinate the provision of access to non-FBI "wanted person" information in NCIC for passport screening purposes.

b. What, if any, obstacles prevent sharing this information, and when will the State Department have access to this information?

Response:

There are no obstacles to the sharing of this information. The TSC has been exporting Terrorist Screening Database (TSDB) data to DOS since the program was implemented on 7/25/05.

**32. What is the average amount of time it takes to translate high priority counter-intelligence audio, which the Inspector General found is not always reviewed within 24 hours?**

**Response:**

At present, the FBI does not collect this information. Based on the OIG report, we are conducting a complete review of our collection of language processing management data to ensure we capture this and other vital information.

**33. I understand from your colleagues in the Bureau that real time translation is likely not possible, but they often speak of "near real time." Translating material on a near simultaneous basis could be critical to preventing an attack, just like listening to suspected criminals on a traditional wiretap can help officials to prevent planned crimes from being carried out. What are the realistic prospects for such material to be translated in something approximating real time?**

**Response:**

Given the volume, velocity, and variety of information collected, near real-time translation of material is not likely absent advances in machine translation capabilities. Near real-time review of critical language material is possible through a combination of priority setting, selection tools, and rudimentary machine translation capabilities.

The FBI is not focused on moving from "near real time" review to "real time" review because it is far more efficient for a linguist to review the foreign language material after it has been recorded. The linguist is able to eliminate any "down time" (such as "dead air" time) by scanning the audio or text rather than listening to or reading the material as it is being produced. In addition, review is conducted in "near real time" because foreign language material is most often routed to the linguist electronically, typically as soon as the phone call or other event ends. Routing the work to the linguist, as opposed to sending the linguist to the collection site, allows the FBI to address even obscure languages quickly and enables a single linguist to process the work from several offices. This would not be possible if we were to place linguists physically at the site of collection to process material in "real time." "Near real time" may be as soon as the target hangs up the phone or up to 24 hours later, depending on the availability of resources proficient in the foreign language.

**34. Your testimony states that the FBI can generally translate its high priority counter-terrorism audio within 24 hours. When the FBI misses that 24 hour target, what is average amount of time that it takes to translate high priority counter-terrorism material?**

**Response:**

The FBI endeavors to review all of its highest priority Foreign Intelligence Surveillance Act (FISA) material within 24 hours of receipt and is generally successful in doing so. The OIG recently conducted tests in eight of the FBI's major translation centers and did find two instances in which material from the highest priority cases was not reviewed within 24 hours (a third instance noted by the OIG involved a negligible amount of material), but in both cases the material was reviewed within 48 hours.

**35. The FBI modified its quality control guidelines in response to the July 2004 audit by the Inspector General. Those new guidelines took effect in December 2004. The July OIG report shows, however, that there is still no nationwide system in place to ensure that FBI field offices perform quality control reviews, or that they monitor the results of reviews. How can you explain this delay?**

**Response:**

At the time of the OIG report, our quality control program had just been implemented and the first reports from that program were not available for OIG review. The OIG did acknowledge that after auditors had completed their field work the FBI provided "documentation showing that it had initiated a nation-wide tracking system and had used the new system to track the first quarterly report received in April 2005." The FBI continues to improve this program and expects to make further progress as we are able to hire and deploy additional personnel. These additional personnel resources will include Regional Program Managers and linguists, who will assist in improving quality control measures and in monitoring the field's compliance with these measures and with other foreign language program initiatives.



**Questions Posed by Senator Feingold**

**36. Thank you for the additional information your office provided regarding the FBI's use of commercial data. When we met earlier this month, you told me that the FBI has contracts with commercial data brokers, but that agents search these databases only for particular information about individuals already under suspicion, and not to look for patterns of behavior that indicate an individual might be a terrorist. Is that a fair characterization?**

**Response:**

That is generally a fair characterization. Commercial databases can be searched by FBI employees for information about individuals and groups in whom the FBI has a valid investigative interest. The FBI does not search commercial databases for patterns of behavior that might be associated with actions of terrorists.

**37. Please provide the Committee with copies of the contracts that the FBI has entered into with commercial data brokers.**

**Response:**

By letter to the Committee dated 4/18/05, we responded to a 3/31/05 letter requesting documents, including active FBI contracts with data brokers. In our response, we noted that on 4/7/05 Judiciary Committee staff received a detailed classified briefing on contracts DOJ and the General Services Administration (GSA) have with data brokers to obtain personal information for investigative purposes. Committee staff also received an unclassified briefing on 3/21/05 from DOJ and FBI officials regarding a recent ChoicePoint compromise, a portion of which addressed DOJ contracts with data brokers. As discussed during the 4/7/05 briefing, the FBI uses the services of Axiom, ChoicePoint, Dun and Bradstreet, iMAPdata, LexisNexis, Seisent (Accurint product), and Westlaw through contracts held by DOJ, GSA, and the Department of the Interior. DOJ provided to the Committee redacted copies of relevant DOJ contracts during the week of 4/11/05.

**38. If the FBI begins to explore the application of data mining technology to commercial data, will you commit to informing the Committee about your plans?**

**Response:**

As the FBI has indicated in previous written responses to this Committee, the FBI does not use public source providers to data mine or run "open-ended" searches for people who might fit a certain pattern. If the FBI should decide to run "open-ended" pattern searches, we will notify the Committee.

**39. Please provide information, in classified form if necessary, regarding any reliance by the FBI on the use of pattern analysis technology or other statistical methods to analyze its own investigative files. Please detail the type of technology employed, the type of data subject to such analysis, any outside contractors involved in this type of analysis, and any guidelines governing such analysis.**

**Response:**

If the term "pattern analysis technology" is used to mean the ability to enter into a computer system a series of general characteristics that operates over a broad set of data to automatically provide a list of those likely to be terrorists, the FBI neither has such a capability nor is seeking to develop one. The FBI does, however, use the IDW to conduct ad hoc and batch queries across documents stored as unstructured data (approximately 50 million documents stored in "flat files," which have no significant structure to permit the identification of data elements) and structured data (approximately 413 million documents containing structure that reveals data elements and permits extraction, transformation, and loading into a database). The set of searchable documents is growing through the addition of new sources of information from both FBI systems and those of other Federal organizations.

These capabilities are provided by commercial products that are integrated into IDW to provide search services, name processing services, and extraction, transformation, and loading services.

**Search services.**

Search services provided by Chiliad products operate over "unstructured" documents (such as text-rich messages, scanned documents, word processing files, and PowerPoint files), and over data extracted and loaded into Oracle databases. The Chiliad product will operate over data in any Open DataBase

Connectivity-compliant relational database management system. Data fusion takes place during indexing and search/analysis. The Chiliad technology suite uses various pattern matching techniques, including contextual searches, probabilistic searches, automatic concept recognition, named entity extraction, and a stemming algorithm.

Search services provided by Convera use Adaptive Pattern Recognition. Processing technology. This technology allows investigators to perform searches for people who have aliases, name variants, or a variety of name spellings, and permits complex searches with complete flexibility in search terms, including any number of wildcards or patterns. Convera also permits the application of pattern recognition technology to search profiling. This technology allows users to register queries using a pattern recognition format, after which all new content flowing into the system is examined for matching patterns and/or wildcards in real-time and users are notified of matches.

Name processing services.

Applications provided by Language Analysis Systems are used to compute probabilities and associated confidence factors for male/female sex determination based on name, to compute probability that a given name is associated with each of 12 nationality groups, and to identify a set of closest matching names in an existing database of names. The computations of probable gender, nationality group, and closest matching names are achieved using pattern matching and statistical analyses of names based on extensive research and analysis of the linguistic and computational properties of names.

Extraction, transformation, and loading services.

IQ Insight is a data profiling tool that can be used to query database tables or flat files to identify patterns, including user-defined patterns (e.g., phone numbers, social security numbers, electronic mail message addresses, names, titles, company names and departments, dates, and addresses). IQ Insight is used to verify that the information in a particular field meets the range, format, and other characteristics expected for that information.

Several contractors assist with IDW maintenance: Scientific Applications International Corporation, Northrop Grumman Corporation - Information Technology Division, and Titan Systems Corporation assist with system operations and maintenance; Chiliad, Convera Corporation, and Informatica Corporation provide vendor support; EW Solutions, Mitretek Systems, and

Buchanan Edwards assist with security and data engineering; and SPAWAR, Eagan, McAllister Associates, Inc., provide program management support.

IDW is an FBI system, and all users must complete mandatory FBI Information Technology Security Awareness training. Users include FBI SAs and analysts, contract analysts serving in operational capacities, and detailees from other federal, state, and local agencies who have been verified as having an operational need for access. Multiple banners (FBI network and IDW) alert users to the restrictions on their use of the IDW system.

Requests to add data sources to IDW must include Privacy Impact Assessments (PIAs), which are reviewed by the FBI Office of the General Counsel (OGC). OGC's reviews of IDW PIAs are then reviewed by the FBI Information Policy Sharing Group, which must approve all sources of data hosted by IDW.

40. The Patriot Act authorized roving taps under the Foreign Intelligence Surveillance Act. That provision did not include an ascertainment requirement, as there is for roving taps under the criminal law. The criminal wiretap statute requires that for roving taps, "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted." 18 U.S.C. § 2518(11)(b)(iv). This ensures that when the order itself does not specify the facility to be tapped, innocent people's phone and computer conversations are not intercepted.

a. Would you object to including a similar ascertainment requirement for FISA roving taps? If your answer is "yes," please explain your reason(s).

Response:

As explained in more detail in the 5/24/05 letter to the Senate Select Committee on Intelligence attached as Enclosure E, the FBI would object to imposing that "ascertainment requirement" for FISA roving wiretaps. The proposed ascertainment requirement would deprive FBI investigators of necessary flexibility in conducting Section 206 roving surveillance. Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world, and are capable of engaging in detailed and extensive counter-surveillance measures. Adding the proposed ascertainment requirement might jeopardize the FBI's ability to conduct surveillance because, in attempting to physically ascertain where the target communication will take place, FBI agents would run the risk of being exposed to sophisticated counter-intelligence efforts.

In addition, the proposed ascertainment requirement would impose significant, unwarranted burdens in cases that are already difficult because of actions by the target that have the effect of thwarting the surveillance. Generally, communications intercepted by criminal Title III surveillance are monitored and minimized contemporaneously by law enforcement personnel. In contrast, communications intercepted pursuant to FISA are generally not contemporaneously monitored. FISA surveillance generally involves after-the-fact review pursuant to minimization procedures approved by the FISA Court (FISC) that limit the acquisition, retention, and dissemination of information about United States persons (thus protecting the privacy of innocent individuals). Under FISA, regardless of whether the surveillance is pursuant to a section 206 order, conversations of "innocent people" are minimized (i.e., not retained in any easily retrievable manner), unless they are talking to or about the authorized target of the surveillance.

Presently, Section 206, together with the practicalities of how surveillance occurs (as discussed below), provides sufficient safeguards to ensure that an innocent person's telephone and computer conversations are not inadvertently intercepted. The target of the roving surveillance must be identified or described in the FISA application with sufficient particularity to permit the FISC to conclude that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Section 206 roving surveillance can be ordered only if the FISC finds, after having determined that the requirements for FISA electronic surveillance have been met, that the actions of the specified target may have the effect of thwarting the surveillance. If the government can demonstrate that to the satisfaction of the FISC, it then obtains a secondary order that can be served on any provider of a facility subsequently determined to be used by the target. As a practical matter, the FBI determines that the target is using a particular facility before it serves the order and begins monitoring the new facility. That determination is, however, very different from a requirement that the FBI must have observed the target near to or on the new facility before it can monitor the resulting communication.

**b. Please explain, in the context of a FISA roving tap, how agents make the decision which facilities to tap. If agents do not ascertain that the target is using a particular facility, how do they decide which facility to tap? How do they decide when to start listening in on the tap?**

**Response:**

This question suggests that there may be a misapprehension about how "roving FISA surveillance" under Section 206 is conducted.

When the FBI determines that the target's actions may have the effect of thwarting surveillance (either by virtue of the target's own practice of switching providers or because the target works for an entity that has an established practice of engaging in tradecraft that thwarts surveillance), the FBI may apply for "roving" electronic surveillance authority. In that event, the court's order would require the known telephone service provider to facilitate the surveillance and would provide the FBI with another order that requires a "specified person" to facilitate the surveillance of the target. The FBI can then serve that second order on any cellular telephone service provider after the FBI has confirmed that the target is using or about to use a new facility, i.e., that he has "roved." Currently, a notice is filed with the FISC identifying the new facility after an order is served on the new provider.

**41. Do you agree that if Congress were to grant the FBI the administrative subpoena authority that you sought at the hearing, the FBI would be highly unlikely to seek a Section 215 order or a National Security Letter ever again? If your answer is no, please describe the circumstances under which the FBI would seek a Section 215 order or an NSL rather than issue an administrative subpoena.**

**Response:**

We do not agree that obtaining administrative subpoena authority would render section 215 orders or National Security Letters (NSLs) obsolete. Generally, the FBI will use the most effective and time-efficient tool available for an investigation, taking into account the type of record sought and our knowledge of the custodian of those records. Administrative subpoena authority would clearly provide a mechanism for obtaining relevant information in national security investigations quickly and without significant expenditure of personnel resources. Although administrative subpoenas might well become the FBI's national security tool of choice, they would not become its only tool. For example, the FBI may well choose to seek a Section 215 order in a very sensitive investigation in which the added imprimatur of a court order to maintain the secrecy of the order is needed (e.g., past experience with the document custodian suggests a lack of care with administrative requests). The FBI may also use a 215 order if it is seeking records that are particularly sensitive, making review by a court before seeking the documents appropriate. The FBI's experience with criminal administrative subpoenas shows that criminal investigators do not limit themselves to one tool, but instead use whatever tool most effectively and efficiently obtains the needed information. We expect our SAs handling national security investigations to exhibit the same initiative in their investigations.

**42. Thank you for your prior responses to questions about the operations of the Terrorist Screening Center (TSC). You explained in those responses that TSC has hired a Privacy Officer to help address complaints about the operation of the TSC watch lists. Please explain the role of the Privacy Officer. Who does the Privacy Officer report to? Does the Privacy Officer have full clearance to review all TSC data?**

**Response:**

The TSC Privacy Officer is formally supervised by the TSC Director, and additionally reports informally to the TSC Chief of Staff to ensure proper coordination of assignments and other matters. The Privacy Officer is responsible for establishing internal policies and procedures to ensure the TSC is in compliance with laws and policies related to the handling of personal information, and for recommending additional policies to ensure that appropriate privacy protections are afforded even in the absence of regulation. The Privacy Officer has full clearance to access all data maintained and used by the TSC in the performance of its mission.

**43. The June Inspector General report evaluating TSC identified problems with the completeness and accuracy of the watch list data, in terms of both omitting known terrorists and including inaccurate information about individuals. What steps is the TSC taking to rectify this problem?**

**Response:**

The TSC is using sophisticated database queries to check for data anomalies, performing record-by-record reviews of the data known to be the most likely to contain inaccuracies, and employing sophisticated custom software to evaluate incoming data against 44 business rules in order to ensure errors do not enter the database.

**44. Would the FBI be willing to allow cleared staff of the Judiciary Committee to visit the TSC to better understand how the watch list process works, how names are added and removed from the list, and how TSC interacts with other agencies?**

**Response:**

On various occasions, the FBI has invited Judiciary Committee members and staff to tour the TSC and obtain a briefing concerning its activities and evolution. We would be pleased to arrange such a visit at the Committee's convenience.

**45. Please provide a list of each federal government agency, department or other entity that relies on the TSC to screen individuals, and the purpose of each screening program. Please include programs in which the government agencies run the names of private sector employees against the watch list.**

**Response:**

The law enforcement components of federal agencies rely on the TSC to screen individuals through the TSDB to identify known or appropriately suspected terrorists, and to provide this information to them on a real-time basis. The initial inquiry by federal law enforcement officials is most often precipitated by a "hit" in the NCIC's VGTOF. The majority of federal encounters in which the TSC is engaged are initiated by the National Targeting Center, which is managed by DHS.

The TSC does not currently run the names of "private sector employees" against the watchlist or any other TSC database unless, of course, they are the subjects of the law enforcement encounters described above. The establishment of programs to support private sector screening is a task for which the DHS is responsible. When those programs are established, the TSC will provide appropriate mechanisms to ensure these screening opportunities are managed properly.

**46. Please provide information about the state and local agencies, departments or other entities that rely on the TSC to screen individuals, and the purposes for which they do so.**

**Response:**

All state and local law enforcement agencies with NCIC access rely on the TSC's TSDB and the NCIC system to identify potential terrorism subjects.

The TSC is a multi-agency organization established under the authority of Homeland Security Presidential Directive 6 to ensure that the names of known or suspected terrorists collected by various U.S. Government agencies are merged into one consolidated list and appropriately shared with federal, state, local, territorial, tribal, and consular authorities, as well as with certain foreign governments. Participants in the TSC include the ODNI, DOJ, DHS, DOS, DoE, and Department of the Treasury. TSDB information is exported to multiple supported systems, including the NCIC's VGTOF. State and local law enforcement authorities are able to query VGTOF for operational direction concerning positively identified known or appropriately suspected terrorists on a "real-time" basis. The FBI's Terrorist Screening Operations Unit (TSOU)



coordinates the operational and investigative response to these inquiries with the appropriate JTTF, which includes representatives from the intelligence community and from the federal, state, and local law enforcement communities. The JTTF conducts liaison with the encountering agency. The TSC also notifies the North American Aerospace Defense Command (NORAD) and the Federal Air Marshal Service (FAMS) of positive encounters during TSC's airline screening process. NORAD is alerted to this information to provide them an opportunity to monitor "Selectee Flights," and FAMS is alerted to permit them to schedule Air Marshals on all "Selectee Flights," making better use of limited resources. These processes have been developed to address gaps within the overall terrorist screening effort and to improve the flow of terrorism-related information.

The ability of the TSC to identify, collect, review, and analyze intelligence from encounters with known or appropriately suspected terrorists increases the effectiveness of the FBI's overall terrorism intelligence base. Daily, this information is shared by the TSC's Tactical Analysis Unit with the FBI's FIGs, which include representatives from the FBI field offices in which they reside and may also include representatives from intelligence agencies and federal, state, and local law enforcement agencies. Through these efforts and those noted above, the TSC has assisted in greatly improving the flow of information between the FBI and state and local law enforcement agencies.

**47. There have been reports that FBI agents registered serious concerns about interrogation techniques they witnessed officials from other agencies or departments employing at Guantanamo Bay.**

**a. When were these concerns brought to your attention?**

**Response:**

Director Mueller does not have a specific recollection as to when he first received this information, but believes that by early 2002 he had determined that FBI Agents participating in interviews overseas should follow FBI protocols.

**b. What steps has the FBI taken within the Administration to oppose the use of coercive interrogations?**

**Response:**

The FBI has clearly communicated its view that rapport-building interview techniques are more effective than coercive or other aggressive techniques.

Testimony of Alberto R. Gonzales, Attorney General of the United States  
and Robert S. Mueller, III, Director, Federal Bureau of Investigation  
United States Department of Justice  
Before the Select Committee on Intelligence  
United States Senate  
April 27, 2005

Chairman Roberts, Vice Chairman Rockefeller, and Members of the Committee:

We are pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, we appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA made by the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from ever happening again.

As we stated in our testimony to the Senate Judiciary Committee, we are open to suggestions for strengthening and clarifying the USA PATRIOT Act, and we look forward to meeting with people both inside and outside of Congress who have expressed views about the Act. However, we will not support any proposal that would undermine our ability to combat terrorism effectively.

**I. FISA Statistics**

First, we would like to talk with you about the use of FISA generally. Since September 11, the volume of applications to the Foreign Intelligence Surveillance Court (FISA court) has dramatically increased.

- In 2000, 1,012 applications for surveillance or search were filed under FISA. As the Department's public annual FISA report sent to Congress on April 1, 2005 states, in 2004 we filed 1,758 applications, a 74% increase in four years.
- Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the FISA court in some substantive way.

**II. Key Uses of FISA Authorities in the War on Terrorism**

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms contained in those measures affect every single application made by the Department for electronic surveillance or physical search of suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to the war on terror that we ask you to reauthorize the provisions of the USA PATRIOT Act scheduled to expire at the end of this

year. Of particular concern is section 206's authorization of multipoint or "roving" wiretaps, section 207's expansion of FISA's authorization periods for certain cases, section 214's revision of the legal standard for installing and using pen register / trap and trace devices, and section 215's grant of the ability to obtain a Court order requesting the production of business records related to national security investigations.

In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 includes a "lone wolf" provision that expands the definition of "agent of a foreign power" to include a non-United States person, who acts alone or is believed to be acting alone and who engages in international terrorism or in activities in preparation therefor. This provision is also scheduled to sunset at the end of this year, and we ask that it be made permanent as well.

#### A. Roving Wiretaps

Section 206 of the USA PATRIOT Act extends to FISA the ability to "follow the target" for purposes of surveillance rather than tie the surveillance to a particular facility and provider when the target's actions may have the effect of thwarting that surveillance. In the Attorney General's testimony at the beginning of this month before the Senate Judiciary Committee, he declassified the fact that the FISA court issued 49 orders authorizing the use of roving surveillance authority under section 206 as of March 30, 2005. Use of roving surveillance has been available to law enforcement for many years and has been upheld as constitutional by several federal courts, including the Second, Fifth, and Ninth Circuits. Some object that this provision gives the FBI discretion to conduct surveillance of persons who are not approved targets of court-authorized surveillance. This is wrong. Section 206 did not change the requirement that before approving electronic surveillance, the FISA court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Without section 206, investigators will once again have to struggle to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Critics of section 206 also contend that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. As a result, they fear that the FBI may violate the communications privacy of innocent Americans. Let me respond to this criticism in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C.

§ 1805(c)(2)(B). Finally, it is important to remember that FISA has always required that the government conduct every surveillance pursuant to appropriate minimization procedures that limit the government's acquisition, retention, and dissemination of irrelevant communications of innocent 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. Section 206 sunsets at the end of this year.

#### **B. Authorized Periods for FISA Collection**

Section 207 of the USA PATRIOT Act has been essential to protecting the national security of the United States and protecting the civil liberties of Americans. It changed the time periods for which electronic surveillance and physical searches are authorized under FISA and, in doing so, conserved limited OIPR and FBI resources. Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases -- which are considerable -- those resources can be devoted instead to other investigative activity as well as conducting appropriate oversight of the use of intelligence collection authorities by the FBI and other intelligence agencies. A few examples of how section 207 has helped are set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law as to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year. It also allows the government to obtain authorization to conduct a physical search of any agent of a foreign power for periods of up to 90 days. Section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the Senate Judiciary Committee, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of applications. Because of section 207's success, we have proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow coverage of all non-U.S. person agents for foreign powers for 120 days initially with each renewal

of such authority allowing continued coverage for one year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission. The WMD Commission agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

### **C. Pen Registers and Trap and Trace Devices**

Some of the most useful, and least intrusive, investigative tools available to both intelligence and law enforcement investigators are pen registers and trap and trace devices. These devices record data regarding incoming and outgoing communications, such as all of the telephone numbers that call, or are called by, certain phone numbers associated with a suspected terrorist or spy. These devices, however, do not record the substantive content of the communications, such as the words spoken in a telephone conversation. For that reason, the Supreme Court has held that there is no Fourth Amendment protected privacy interest in information acquired from telephone calls by a pen register. Nevertheless, information obtained by pen registers or trap and trace devices can be extremely useful in an investigation by revealing the nature and extent of the contacts between a subject and his confederates. The data provides important leads for investigators, and may assist them in building the facts necessary to obtain probable cause to support a full content wiretap.

Under chapter 206 of title 18, which has been in place since 1986, if an FBI agent and prosecutor in a criminal investigation of a bank robber or an organized crime figure want to install and use pen registers or trap and trace devices, the prosecutor must file an application to do so with a federal court. The application they must file, however, is exceedingly simple: it need only specify the identity of the applicant and the law enforcement agency conducting the investigation, as well as "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." Such applications, of course, include other information about the facility that will be targeted and details about the implementation of the collection, as well as "a statement of the offense to which the information likely to be obtained . . . relates," but chapter 206 does not require an extended recitation of the facts of the case.

In contrast, prior to the USA PATRIOT Act, in order for an FBI agent conducting an intelligence investigation to obtain FISA authority to use the same pen register and trap and trace device to investigate a spy or a terrorist, the government was required to file a complicated application under title IV of FISA. Not only was the government's application required to include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General," it also had to include the following:

information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with—

(A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or

(B) a foreign power or agent of foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

Thus, the government had to make a much different showing in order obtain a pen register or trap and trace authorization to find out information about a spy or a terrorist than is required to obtain the very same information about a drug dealer or other ordinary criminal. Sensibly, section 214 of the USA PATRIOT Act simplified the standard that the government must meet in order to obtain pen/trap data in national security cases. Now, in order to obtain a national security pen/trap order, the applicant must certify "that the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities." Importantly, the law requires that such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Section 214 should not be permitted to expire and return us to the days when it was more difficult to obtain pen/trap authority in important national security cases than in normal criminal cases. This is especially true when the law already includes provisions that adequately protect the civil liberties of Americans. I urge you to re-authorize section 214.

#### **D. Access to Tangible Things**

Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the First Amendment to the Constitution. The Attorney General also declassified earlier this month the fact that the FISA Court has issued 35 orders requiring the production of tangible things under section 215 from the date of the effective date of the Act through March 30th of this year. None of those orders was issued to libraries and/or booksellers, and none was for medical or gun records. The provision to date has been used only to order the production of driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices.

Similar to a prosecutor in a criminal case issuing a grand jury subpoena for an item relevant to his investigation, so too may the FISA Court issue an order requiring the production of records or items that are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to judicial oversight before they are issued – unlike grand jury subpoenas. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the order on a recipient. In contrast, grand jury subpoenas are subject to judicial review only if they are challenged by the recipient. Section 215 orders are also subject to the same standard as grand jury subpoenas – a relevance standard.

Section 215 has been criticized because it does not exempt libraries and booksellers. The absence of such an exemption is consistent with criminal investigative practice. Prosecutors have always been able to obtain records from libraries and bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. Last year, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

Concerns that section 215 allows the government to target Americans because of the books they read or websites they visit are misplaced. The provision explicitly prohibits the government from conducting an investigation of a U.S. person based solely upon protected First Amendment activity. 50 U.S.C. § 1861(a)(2)(B). However, some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points. Section 215 also is scheduled to sunset at the end of this year.

#### **E. The “Wall”**

Before the USA PATRIOT Act, applications for orders authorizing electronic surveillance or physical searches under FISA had to include a certification from a high-ranking Executive Branch official that “the purpose” of the surveillance or search was to gather foreign intelligence information. As interpreted by the courts and the Justice Department, this requirement meant that the “primary purpose” of the collection had to be to obtain foreign intelligence information rather

than evidence of a crime. Over the years, the prevailing interpretation and implementation of the “primary purpose” standard had the effect of sharply limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government’s purpose for using FISA at least in part by examining the nature and extent of such coordination, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence collection, had become the primary purpose of the surveillance or search.

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel even more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation’s primary purpose. The procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement personnel became more limited in practice than was allowed in reality. A perception arose that improper information sharing could end a career, and a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Sections 218 and 504 of the USA PATRIOT Act helped to bring down this “wall” separating intelligence and law enforcement officials. They erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel. They also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 of the USA PATRIOT Act eliminated the “primary purpose” requirement. Under section 218, the government may conduct FISA surveillance or searches if foreign intelligence gathering is a “significant” purpose of the surveillance or search. This eliminated the need for courts to compare the relative weight of the “foreign intelligence” and “law enforcement” purposes of the surveillance or search, and allows increased coordination and sharing of information between intelligence and law enforcement personnel. Section 218 was upheld as constitutional in 2002 by the FISA court of Review. This change, significantly, did not affect the government’s obligation to demonstrate that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Section 504 – which is not subject to sunset – buttressed section 218 by specifically amending FISA to allow intelligence officials conducting FISA surveillances or searches to “consult” with federal law enforcement officials to “coordinate” efforts to investigate or protect against international terrorism, espionage, and other foreign threats to national security, and to clarify that such coordination “shall not” preclude the



certification of a "significant" foreign intelligence purpose or the issuance of an authorization order by the FISA court.

The Department moved aggressively to implement sections 218 and 504. Following passage of the Act, the Attorney General adopted new procedures designed to increase information sharing between intelligence and law enforcement officials, which were affirmed by the FISA court of Review on November 18, 2002. The Attorney General has also issued other directives to further enhance information sharing and coordination between intelligence and law enforcement officials. In practical terms, a prosecutor may now consult freely with the FBI about what, if any, investigative tools should be used to best prevent terrorist attacks and protect the national security. Unlike section 504, section 218 is scheduled to sunset at the end of this year.

The increased information sharing facilitated by the USA PATRIOT Act has led to tangible results in the war against terrorism: plots have been disrupted; terrorists have been apprehended; and convictions have been obtained in terrorism cases. Information sharing between intelligence and law enforcement personnel, for example, was critical in successfully dismantling a terror cell in Portland, Oregon, popularly known as the "Portland Seven," as well as a terror cell in Lackawanna, New York. Such information sharing has also been used in the prosecution of several persons involved in al Qaeda drugs-for-weapons plot in San Diego, two of whom have pleaded guilty; nine associates in Northern Virginia of a violent extremist group known as Lashkar-e-Taiba that has ties to al Qaeda, who were convicted and sentenced to prison terms ranging from four years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged and convicted for conspiring to provide material support to al Qaeda and HAMAS; Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury; and Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation, who had a long-standing relationship with Osama Bin Laden and pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from his charity organization to support Islamic militant groups in Bosnia and Chechnya. Information sharing between intelligence and law enforcement personnel has also been extremely valuable in a number of other ongoing or otherwise sensitive investigations that we are not at liberty to discuss today.

While the "wall" primarily hindered the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the USA PATRIOT Act, often hampered law enforcement officials from sharing information with intelligence personnel and others in the government responsible for protecting the national security. Federal law, for example, was interpreted generally to prohibit federal prosecutors from disclosing information from grand jury testimony and criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were actually assisting with the criminal investigation. Sections 203(a) and (b) of the USA PATRIOT Act, however, eliminated these obstacles to information sharing by allowing for the dissemination of that information to assist Federal law enforcement, intelligence, protective, immigration, national defense, and national

security officials in the performance of their official duties, even if their duties are unrelated to the criminal investigation. (Section 203(a) covers grand jury information, and section 203(b) covers wiretap information.) Section 203(d), likewise, ensures that important information that is obtained by law enforcement means may be shared with intelligence and other national security officials. This provision does so by creating a generic exception to any other law purporting to bar Federal law enforcement, intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation. Indeed, section 905 of the USA PATRIOT Act requires the Attorney General to expeditiously disclose to the Director of Central Intelligence foreign intelligence acquired by the Department of Justice in the course of a criminal investigation unless disclosure of such information would jeopardize an ongoing investigation or impair other significant law enforcement interests.

The Department has relied on section 203 in disclosing vital information to the intelligence community and other federal officials on many occasions. Such disclosures, for instance, have been used to assist in the dismantling of terror cells in Portland, Oregon and Lackawanna, New York and to support the revocation of suspected terrorists' visas.

Because two provisions in section 203: sections 203(b) and 203(d) are scheduled to sunset at the end of the year, we provide below specific examples of the utility of those provisions. Examples of cases where intelligence information from a criminal investigation was appropriately shared with the Intelligence Community under Section 203(d) include:

- Information about the organization of a violent jihad training camp including training in basic military skills, explosives, weapons and plane hijackings, as well as a plot to bomb soft targets abroad, resulted from the investigation and criminal prosecution of a naturalized United States citizen who was associated with an al-Qaeda related group;
- Travel information and the manner that monies were channeled to members of a seditious conspiracy who traveled from the United States to fight alongside the Taliban against U.S. and allied forces;
- Information about an assassination plot, including the use of false travel documents and transporting monies to a designated state sponsor of terrorism resulted from the investigation and prosecution of a naturalized United States citizen who had been the founder of a well-known United States organization;
- Information about the use of fraudulent travel documents by a high-ranking member of a designated foreign terrorist organization emanating from his criminal investigation and prosecution revealed intelligence information about the manner and means of the terrorist group's logistical support network which was shared in order to assist in protecting the lives of U.S. citizens;

- The criminal prosecution of individuals who traveled to, and participated in, a military-style training camp abroad yielded intelligence information in a number of areas including details regarding the application forms which permitted attendance at the training camp; after being convicted, one defendant has testified in a recent separate federal criminal trial about this application practice, which assisted in the admissibility of the form and conviction of the defendants; and
- The criminal prosecution of a naturalized U.S. citizen who had traveled to an Al-Qaeda training camp in Afghanistan revealed information about the group's practices, logistical support and targeting information.

Title III information has similarly been shared with the Intelligence Community through section 203(b). The potential utility of such information to the intelligence and national security communities is obvious: suspects whose conversations are being monitored without their knowledge may reveal all sorts of information about terrorists, terrorist plots, or other activities with national security implications. Furthermore, the utility of this provision is not theoretical: the Department has made disclosures of vital information to the intelligence community and other federal officials under section 203(b) on many occasions, such as:

- Wiretap interceptions involving a scheme to defraud donors and the Internal Revenue Service and illegally transfer monies to Iraq generated not only criminal charges but information concerning the manner and means by which monies were funneled to Iraq; and
- Intercepted communications, in conjunction with a sting operation, led to criminal charges and intelligence information relating to money laundering, receiving and attempting to transport night-vision goggles, infrared army lights and other sensitive military equipment relating to a foreign terrorist organization.

Section 203 is also critical to the operation of the National Counterterrorism Center. The FBI relies upon section 203(d) to provide information obtained in criminal investigations to analysts in the new National Counterterrorism Center, thus assisting the Center in carrying out its vital counterterrorism missions. The National Counterterrorism Center represents a strong example of section 203 information sharing, as the Center uses information provided by law enforcement agencies to produce comprehensive terrorism analysis; to add to the list of suspected terrorists on the TIPOFF watchlist; and to distribute terrorism-related information across the federal government.

In addition, last year, during a series of high-profile events – the G-8 Summit in Georgia, the Democratic Convention in Boston and the Republican Convention in New York, the November 2004 presidential election, and other events – a task force used the information sharing provisions under Section 203(d) as part and parcel of performing its critical duties. The 2004 Threat Task Force was a successful inter-agency effort where there was a robust sharing of information at all levels of government.

## **F. Protecting Those Complying with FISA Orders**

Often, to conduct electronic surveillance and physical searches, the United States requires the assistance of private communications providers to carry out such court orders. In the criminal context, those who assist the government in carrying out wiretaps are provided with immunity from civil liability. Section 225, which is set to sunset, provides immunity from civil liability to communication service providers and others who assist the United States in the execution of FISA orders. Prior to the passage of the USA PATRIOT Act, those assisting in the carrying out of FISA orders enjoyed no such immunity. Section 225 simply extends the same immunity that has long existed in the criminal context to those who assist the United States in carrying out orders issued by the FISA court. Providing this protection to communication service providers for fulfilling their legal obligations helps to ensure prompt compliance with FISA orders.

### **CONCLUSION**

It is critical that the elements of the USA PATRIOT Act subject to sunset in a matter of months be renewed. Failure to do so would take the Intelligence Community and law enforcement back to a time when a full exchange of information was not possible and the tools available to defend against terrorists were inadequate. This is unacceptable. The need for constant vigilance against terrorists wishing to attack our nation is real, and allowing USA PATRIOT Act provisions to sunset would damage our ability to prevent such attacks.

We thank the Committee for the opportunity to discuss the importance of the USA PATRIOT Act to this nation's ongoing war against terrorism. This Act has a proven record of success in protecting the American people. Provisions subject to sunset must be renewed. We look forward to working with the Committee in the weeks ahead. We appreciate the Committee's close attention to this important issue. We would be pleased to answer any questions you may have. Thank you.

**Statement of  
James B. Comey  
Deputy Attorney General  
United States Department of Justice  
Before the  
Committee on the Judiciary  
United States House of Representatives**

**June 8, 2005**

Introduction

Good Morning. Chairman Sensenbrenner, Ranking Member Conyers and Members of the Committee, it is my pleasure to appear before you today to discuss the USA PATRIOT Act. Thank you for allowing me the opportunity to discuss the important tools contained in that Act. As I have said many times before Members and Committees of both houses of Congress, and all over the country, when it comes to the USA PATRIOT Act, I believe that the angel is in the details and that if we engage in conversation and shed daylight on how the Department of Justice has used the important tools in the Act, more people will come to see that the tools are simple, constitutional, and just plain sensible.

The Administration is fighting the War against Terror both at home and abroad using all the lawful tools at our disposal. Survival and success in this struggle demand that the Department continuously improve its capabilities to protect Americans from a relentless enemy. The Department will continue to seek the assistance of Congress as it builds a culture of prevention and ensures that our government's resources are dedicated to defending the safety and security of the American people.

I will never forget, as I know the Members of this Committee will not forget, the thousands of our fellow citizens that were murdered at the World Trade Center, the Pentagon and a field in rural Pennsylvania. Nearly four years have passed since that tragic day and, in large part due to the tremendous efforts of our federal, state and local law enforcement as well as the Intelligence Community, our country has been spared another attack of that magnitude. But our success presents a new challenge. How do we bring voice to victims that were never murdered, to family members who have not lost a loved one? How do we explain to Congress and the American people these "ghost pains?" This is the continuing challenge of law enforcement in our country. When we are faced with rising crime and victimization rates, it is easy to point to those in need of our protection to justify our requests for tools to protect our citizens. But when we are successful in our efforts, when our hard work and relentlessness pays off, it becomes more difficult to convince the people to let us keep those tools.

Mr. Chairman, as a career prosecutor, and now in my role as Deputy Attorney General, I have heard many times the question of when will we next break up a terror cell moments before implementation of a devastating plot. But let me tell you, as a prosecutor, you don't want to be there. You want to catch a terrorist with his hands on the check instead of his hands on the bomb. You want to be many steps ahead of the devastating event. The way we do that is

through preventive and disruptive measures, by using investigative tools to learn as much as we can as quickly as we can and then incapacitating a target at the right moment. Tools such as enhanced information sharing mechanisms, roving surveillance, pen registers, requests for the production of business records, and delayed notification search warrants allow us to do just that.

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

I'd next like to discuss the material support statutes, which are the cornerstone of our prosecution efforts. The first material support case to be tried before a jury involved a group of Hizballah operatives in Charlotte, North Carolina found to have been involved in a massive inter-state cigarette smuggling and tax evasion scheme. The investigation uncovered a related plot in which some of these defendants were procuring dual-use items at the instructions of Hizballah leaders in Lebanon. This indictment, which involved RICO and material support charges, resulted in the conviction of 20 people. The Charlotte prosecution was upheld by the Fourth Circuit Court of Appeals (*United States v. Hammoud*, 4<sup>th</sup> Cir., September 8, 2004; remanded for resentencing in light of *Booker*). Since then, "material support" charges have been used against other cigarette smuggling plots in Detroit. We have successfully prosecuted *al Qaeda* supporters in Portland and Alexandria, and Hizballah supporters in Detroit and Charlotte. We have convicted persons involved in *jihād* training activities in Buffalo, Seattle, and Alexandria.

Indeed, prior to the attacks of 9/11, 17 persons in four different judicial districts were charged with offenses relating to material support to terrorists and terrorist organizations. Since then, however, 135 people in at least 25 different judicial districts have been charged with material support-related offenses. Of the 152 people charged both before and since 9/11, 70 have been convicted or pleaded guilty, and many more are still awaiting trial.

Our prosecution of those who seek to provide material support continues including most recently a on April 27, 2005, a New Jersey federal jury convicted Hemant Lakhani, a United Kingdom national, of attempting to provide material support to terrorists for his role in trying to sell an antiaircraft missile to a man whom he believed represented a terrorist group intent on shooting down a United States commercial airliner. On April 22, 2005, in the Eastern District of Virginia, Zacarias Moussaoui pled guilty to six counts of conspiracy, acknowledging his role in assisting *al Qaeda*. Also on April 22, 2005, a jury convicted Ali Al-Timimi, a speaker and spiritual leader in Northern Virginia, in the second phase of the Northern Virginia jihad case involving a group of individuals who were encouraged and counseled by Al-Timimi to go to Pakistan to receive military training from Lashkar-e-Taiba, which has ties to the *al Qaeda* terrorist network, in order to be able to fight against American troops. The first phase of the

prosecution involved convictions under the material support statutes; Al-Timimi's firearms convictions were predicated, in part, on the material support statutes. And there are many more examples due to our continuing efforts to ensure the safety of the American people.

#### Foreign Intelligence Surveillance Act

The authorities contained in the Foreign Intelligence Surveillance Act (FISA) have been critical to the Department's efforts to combat terrorism. Since September 11, 2001, the volume of applications to the Foreign Intelligence Surveillance Court (FISA Court) has dramatically increased. In 2000, 1,012 applications for surveillance or searches were filed under FISA. By comparison, in 2004 we filed 1,758 applications; this represents a 74% increase in four years. Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the FISA Court in some substantive way.

In enacting the USA PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with tools that it has used regularly and effectively in its war on terrorism. The reforms in those measures affect every single application made by the Department for electronic surveillance or physical searches authorized under FISA regarding suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to winning the war on terror that the Department asks you to reauthorize those USA PATRIOT Act provisions scheduled to expire at the end of this year.

For example, section 207 of the USA PATRIOT Act governs the authorized periods for FISA collection and has been essential to protecting both the national security of the United States and the civil liberties of Americans. It changed the time periods for which some electronic surveillance and physical searches are authorized under FISA, and, in doing so, conserved limited resources of both the FBI and the Department's Office of Intelligence Policy and Review (OIPR). Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases -- which are considerable -- those resources are now devoted to other investigative activities as well as conducting appropriate oversight of the use of intelligence collection authorities at the FBI and other intelligence agencies. A few examples of how section 207 has helped the Department are set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the

government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident-alién members of international groups for initial periods of 120 days, with extensions for periods of up to one year. It also allows the government to obtain authorization to conduct physical searches targeting any agent of a foreign power for periods of up to 90 days. Section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods for electronic surveillance and physical search equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the House Judiciary Committee, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of FISA applications. This figure does not include the time saved by agents and attorneys at the FBI. Because of section 207's success, the Department has proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow initial coverage of any non-U.S. person agent of a foreign power for 120 days with each renewal of such authority allowing continued coverage for one year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the bipartisan WMD Commission. The WMD Commission agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

#### Access to Tangible Things

Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the First Amendment to the Constitution. The Attorney General recently declassified the fact that the FISA Court has issued 35 orders requiring the production of tangible things under section 215 from the effective date of the Act through March 30th of this year. None of those orders were issued to libraries and/or booksellers, and none were for medical or gun records. The provision to date has been used only to order the production of driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses for telephone numbers captured through court-authorized pen register devices.



Similar to a prosecutor in a criminal case issuing a grand jury subpoena for an item relevant to his investigation, so too can an investigator obtain an order from the FISA Court requiring production of records or items that are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to judicial oversight before they are issued – unlike grand jury subpoenas. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the order on a recipient. In contrast, grand jury subpoenas are subject to judicial review only if they are challenged by the recipient. Section 215 orders are also subject to a similar standard as are grand jury subpoenas – a relevance standard.

Section 215 has been criticized by some because it does not exempt libraries and booksellers. The absence of such an exemption is consistent with criminal investigative practice. Prosecutors have always been able to obtain records from libraries and bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. Last year, a member of a terrorist group closely affiliated with *al Qaeda* used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

Concerns that section 215 allows the government to target Americans because of the books they read or websites they visit are misplaced. The provision explicitly prohibits the government from conducting an investigation of a U.S. person based solely upon protected First Amendment activity. 50 U.S.C. § 1861(a)(2)(B). And, as the Attorney General has made clear, we have no interest in the reading habits of ordinary Americans. However, some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, would support amendments to section 215 to clarify these points. Section 215 also is scheduled to sunset at the end of this year.

The right of a recipient to challenge a production order must, however, be distinguished from a potential right of a third party to suppress information obtained from the recipient—a right not normally afforded in criminal proceedings. This, for example, is true in the case of grand jury subpoenas. *See, e.g., United States v. Miller*, 425 U.S. 435 (1976) (holding that bank customer had no standing to challenge the validity of grand jury subpoenas issued to a bank for

his records). Similarly, a defendant in a criminal proceeding has no constitutional right to suppress evidence obtained in a search of someone else's property, even if that search was conducted unlawfully. *See, e.g., Rakas v. Illinois*, 439 U.S. 128 (1978) (passengers in car have no standing to suppress evidence obtained in allegedly illegal search and seizure of car); *see also Wong Sun v. United States*, 371 U.S. 471 (1963) (defendant may not suppress evidence obtained as a product of statement made by co-defendant incident to an unlawful arrest, even though the evidence was inadmissible against co-defendant); *United States v. Mendoza-Burciaga*, 981 F.2d 192 (5th Cir. 1992) (driver of a truck has standing to challenge a search of the truck, but a passenger does not).

While the Department supports the aforementioned clarifying amendments to section 215, the Department is very concerned by proposals currently pending before Congress which would require the government to show "specific and articulable facts" that the records sought through a section 215 order pertain to a foreign power or agent of a foreign power. Such a requirement would disable the government from using a section 215 order at the early stages of an investigation, which is precisely when such an order is most useful.

Consider, for example, a case where a known terrorist is observed having dinner with an unknown individual at a hotel. Currently, investigators may use section 215 to obtain the unknown individual's hotel records so that he may be identified and then investigated further so that the government may find out if he is also involved in terrorism. It is important to remember that terrorists and spies are generally trained to camouflage their dangerous activities and thus even an innocent conversation or encounter may look benign to an untrained observer. But our agents must be enabled to, when conducting surveillance, follow up on individuals associating with known *al Qaeda* operatives. Such a use of section 215, however, would not be permissible if the standard were changed from relevance to one of specific and articulable facts that the records pertain to a foreign power or agent of a foreign power. This is because investigators in this hypothetical do not yet know whether the unknown individual is a terrorist or spy. Indeed, that is exactly the question that investigators are trying to answer by using section 215.

#### Pen Register and Trap-and-Trace Devices

Some of the most useful, and least intrusive, investigative tools available to both intelligence and law enforcement investigators are pen registers and trap and trace devices. These devices record data regarding incoming and outgoing communications, such as all of the telephone numbers that call, or are called by, certain phone numbers associated with a suspected terrorist or spy. These devices, however, are not used to record the substantive content of the communications. For that reason, the Supreme Court has held that there is no Fourth Amendment protected privacy interest in information acquired from telephone calls by a pen register. Nevertheless, information obtained by pen registers or trap and trace devices can be extremely useful in an investigation by revealing the nature and extent of the contacts between a

subject and his confederates. The data provides important leads for investigators, and may assist them in building the facts necessary to obtain probable cause to support a full content wiretap.

Under chapter 206 of title 18, which has been in place since 1986, if an FBI agent and prosecutor in a criminal investigation of a bank robber or an organized crime figure want to install and use pen registers or trap and trace devices, the prosecutor must file an application to do so with a federal court. The application they must file, however, is exceedingly simple: it need only specify the identity of the applicant and the law enforcement agency conducting the investigation, as well as "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." Such applications, of course, include other information about the facility that will be targeted and details about the implementation of the collection, as well as "a statement of the offense to which the information likely to be obtained . . . relates," but chapter 206 does not require an extended recitation of the facts of the case.

In contrast, prior to the USA PATRIOT Act, in order for an FBI agent conducting an intelligence investigation to obtain FISA authority to use the same pen register and trap and trace device to investigate a spy or a terrorist, the government was required to file a complicated application under title IV of FISA. Not only was the government's application required to include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General," it also had to include the following:

information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with—

(A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or

(B) a foreign power or agent of foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

Thus, the government had to make a much different showing in order obtain a pen register or trap and trace authorization to find out information about a spy or a terrorist than is required to obtain the very same information about a drug dealer or other ordinary criminal. Sensibly, section 214 of the USA PATRIOT Act simplified the standard that the government

must meet in order to obtain pen/trap data in national security cases. Now, in order to obtain a national security pen/trap order, the applicant must certify "that the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities." Importantly, the law requires that such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Section 214 should not be permitted to expire and return us to the days when it was more difficult to obtain pen/trap authority in important national security cases than in normal criminal cases. This is especially true when the law already includes provisions that adequately protect the civil liberties of Americans. I therefore urge you to re-authorize section 214.

Proposals currently before the Congress would raise the standard for obtaining a pen register or trap and trace device – both in the criminal investigative and FISA contexts – from relevance to "specific and articulable facts." Like subpoenas, pen registers and trap and trace devices are not as intrusive as other investigative techniques and often are used as the building blocks of an investigation. Federal courts have held that the Constitution does not even require a court order for such a device to be installed (though federal statute does so require) because of the lower expectation of privacy that attaches to the numbers dialed to and from a telephone. Imposing a specific and articulable facts standard on pen registers/trap and trace devices would hamper investigations just as imposing such a standard on section 215 orders would.

#### Information Sharing

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. To be sure, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was allowed in theory under the Department's procedures. Due both to confusions about when sharing was permitted and to a perception that improper information sharing could end a career, a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Through enactment of sections 203 and 218, the USA PATRIOT Act helped bring down this "wall" separating intelligence officers from law enforcement agents. It not only erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel, but it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

The Department's efforts to increase coordination and information sharing between intelligence and law enforcement officers, which were made possible by the USA PATRIOT Act, have yielded extraordinary dividends by enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases. For example, the removal of the barriers separating intelligence and law enforcement personnel played an important role in investigations and prosecutions of the Portland Seven, Sami Al-Arian, the Virginia Jihad case and numerous others.

Some have voiced the concern that under section 218 of the USA PATRIOT Act the government may utilize FISA surveillance when its primary purpose is to investigate and prosecute crimes unrelated to foreign intelligence. For example, the government, in obtaining a surveillance order targeting an agent of a foreign power, may have a significant purpose of obtaining foreign intelligence information but its primary purpose would be to investigate and prosecute that agent of a foreign power for a crime unrelated to foreign intelligence, such as tax fraud. This interpretation of FISA, however, has been clearly rejected by the FISA Court of Review, which observed that it would be "an anomalous reading" of section 218. The manifestation of such a primary purpose, the FISA Court of Review has stated, "would disqualify an application" under FISA. According to the court, this is because "the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes." *In re Sealed Case*, 310 F.3d 717, 736 (FISCR 2002).

#### Roving Wiretaps

Another important tool provided in the USA PATRIOT Act was provided by section 206, which allows the FISA Court to authorize "roving" surveillance of a terrorist or spy. This "roving" wiretap order attaches to a particular target rather than a particular phone or other communication facility. Since 1986, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering. Section 206 simply authorized the same techniques used to investigate ordinary crimes to be used in national security investigations. Before the USA PATRIOT Act, the use of roving wiretaps was not available under FISA. Therefore, each time a suspect changed communication providers, investigators had to return to the FISA Court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap. International terrorists and foreign intelligence officers are trained to thwart surveillance by

changing communication facilities just prior to important meetings or communications. This provision therefore has put investigators in a better position to counter the actions of spies and terrorists who are trained to thwart surveillance. This is a tool that we do not use often, but when we use it, it is critical. As of March 30, 2005, it had been used 49 times.

Section 206 also contains important privacy safeguards. Under Section 206, the target of roving surveillance must be identified or described in the order. Therefore, section 206 is always connected to a particular target of surveillance. Even if the government is not sure of the actual identify of the target of the wiretap, FISA nonetheless requires the government to provide "a description of the target of the electronic surveillance" to the FISA Court prior to obtaining a roving surveillance order. Under Section 206, furthermore, before approving a roving surveillance order, the FISA Court must find that there is probable cause to believe the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or a spy. The description of the target must, therefore, be sufficiently detailed for the FISA Court to find probable cause that the target is either a foreign power or an agent of a foreign power. Roving surveillance under section 206 also can be ordered only after a FISA Court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance. Moreover, Section 206 in no way altered the FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons. A number of federal courts, including the Second, Fifth, and Ninth Circuits, have squarely ruled that "roving" wiretaps are perfectly consistent with the Fourth Amendment. No court of appeals has reached a contrary conclusion.

Proposals currently pending before Congress would require the government to know the "identity" of the target in order to obtain a roving wiretap. This limitation would be problematic in the FISA context, in which we may be dealing with spies and terrorists trained to cloak their identities. If the government is able to find a description of the target sufficiently specific to allow the FISA Court to find probable cause that the target is an agent of a foreign power and may take action to thwart surveillance, the FISA Court should be able to authorize roving surveillance of that target.

Proposals in Congress also would require that the presence of the target at a particular telephone be "ascertained" by the person conducting the surveillance before the phone could be surveilled. This is a stricter standard than is required in the criminal context and would be impracticable in the FISA context, in which surveillance is usually done continually on a targeted phone and later translated and culled pursuant to minimization procedures. Moreover, such a requirement would be exceptionally risky in a world where terrorists and spies are trained extensively in counter-surveillance measures.

### National Security Letters

Currently, NSLs, which are similar to administrative subpoenas, are issued for certain types of documents "relevant" to international terrorism or espionage investigations. Provisions currently before Congress would amend each existing NSL authority to impose one or more "specific and articulable facts" requirements. For each type of record, the government would be required to show specific and articulable facts that the records sought "pertain to a foreign power or agent of a foreign power." Additional specific and articulable facts requirements would be imposed with respect to other types of information. For example, with respect to telephone subscriber information, the government would have to show specific and articulable facts that the subscriber's communications devices "have been used" in communication with certain categories of individuals. These standards would significantly reduce the usefulness of NSLs for the same reason that a heightened standard of proof would diminish the usefulness of section 215.

### Delayed Notification Search Warrants

Section 213 of the USA PATRIOT Act brought national uniformity to a court-approved law enforcement tool that had been in existence for decades and has been relied on by investigators and prosecutors in limited but essential circumstances. While there has been much discussion about this provision, there remain many misconceptions about this tool. The concept of rolling back delayed notification search warrants in any manner concerns me and demonstrates, I believe, a misunderstanding of how our criminal justice system works. Approval to delay notification of a search warrant is granted only after a federal judge finds reasonable cause to believe that immediate notification of execution of a search warrant would bring one of five enumerated adverse results including destruction of evidence, witness tampering, or serious jeopardy to an investigation. It is important to remember that judicial approval for the underlying search warrant is also required and remains governed by the probable cause standard. Nothing in the USA PATRIOT Act changed that. Also, notice is always provided to the target of the search, it is only delayed temporarily.

Section 213, like other provisions of the USA PATRIOT Act, is one tool we use in our efforts to combat terrorism. Although the Department has used this provision at least 18 times in terrorism-related investigations, it is true that this provision is used more frequently in non-terrorism contexts, particularly large, sensitive drug investigations, as it was for decades before the USA PATRIOT Act. This should not undermine the fact that it is an important tool to law enforcement and should not be limited to only the national security context. Indeed, the use of delayed notice search warrants in non-terrorism cases is consistent with Congressional intent – section 213 was never limited to terrorism cases. Some opponents of this tool also attempt to hold our agents' and prosecutors professionalism against us, by pointing to statistics showing that federal judges have never denied a request for a delayed notification search warrant. At the

Department of Justice, we have the highest expectations for our professionals. Every prosecutor pushes for more than the bare minimum and takes great care to lay out facts and circumstances in application for a search warrant that meet or exceed the probable cause requirement. In addition, the record reflects the fact that the Department has judiciously sought delayed notification search warrants as they comprise fewer than 2 in 1000 search warrants issued nationwide.

Some opponents of our use of section 213 would strike one essential justification for delayed notices search warrants, that immediate notice would "seriously jeopardize an investigation" from the statute. This would hamper criminal investigations in circumstances where immediate notice would cause an adverse effect not otherwise listed in the statute. For example, if the "seriously jeopardize" prong were eliminated, notice could not be delayed even if immediate notice of a search would jeopardize an ongoing and productive Title III wiretap. I'd like to highlight one example of where the "seriously jeopardizing an investigation" prong was the sole "adverse result" used to request delayed notice.

In 2004 the Justice Department executed three delayed notice searches as part of an OCDETF investigation of a major drug trafficking ring that operated in the Western and Northern Districts of Texas. 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. The original delay approved by the court in this case was for 60 days. The Department sought two extensions, one for 60 days and one for 90 days, both of which were approved.

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 which would have alerted the criminals to the existence of 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 this 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 notice has been given in all cases.



In addition, certain proposals currently before Congress would limit the discretion of a federal judge in granting the initial periods of delay other than seven days. It would allow extensions in 21-day increments, but only if the Attorney General, DAG, or Associate Attorney General personally approved the application for an extension. Requiring the government to go back to court after seven days – even where the court would have found a longer period of delay reasonable under the circumstances – would unduly burden law enforcement and judicial resources. And although the provision for a 21-day extension period is better than the 7-day period previously suggested by critics, requiring personal approval by the AG, DAG, or Associate would be impractical and unnecessarily burdensome. Currently, the length of delay is decided on a case-by-case basis by a federal judge familiar with the facts of a particular investigation. The Department believes that this system has worked well and should not be replaced by a one-size-fits-all statutory time limit.

#### Allegations of Abuse

In addition, the Department of Justice remains very concerned about any allegations of abuse of the tools provided in the USA PATRIOT Act. I am pleased that the Congress takes its oversight role seriously and has been attempting to address any relevant allegations. As Congress decides the fate of the tools contained in the Act, I 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 her request for information regarding alleged “abuses” of the USA PATRIOT Act. Senator Feinstein requested that the Department review these allegations. 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.

For example, the ACLU’s letter alleged that the “Patriot Act [was used] to secretly search the home of Brandon Mayfield, a Muslim attorney whom the government wrongly suspected, accused and detained as a perpetrator of the Madrid train bombings.” Mr. Mayfield’s home was searched with the approval of a federal judge because the available information, including an erroneous finger-print match, gave investigators probable cause to believe that he was involved in the terrorist bombings in Madrid -- the search was not on account of any new authority created by the USA PATRIOT Act or any abuse of the Act.

The ACLU’s allegation regarding Mr. Mayfield seems to be based in part on the mistaken idea that the search of Mr. Mayfield’s home was conducted pursuant to section 213 of the USA PATRIOT Act. That is not correct. The search was conducted pursuant to the Foreign Intelligence Surveillance Act under an authority that has existed in the FISA statute since 1995. Because the search was conducted under a FISA Court order, some of the USA PATRIOT Act

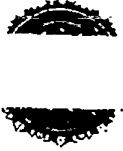
provisions that amended FISA or relate to intelligence investigations may have been implicated or "used" in some sense of that word. That does not in any way mean that these USA PATRIOT Act provisions were misused. The Department would be happy to share other information from our letter to Senator Feinstein with the Committee.

Moreover, last month, the Department of Justice's Inspector General, Glenn A. Fine, testified before the Subcommittee on Crime, Terrorism and Homeland Security about section 1001 of the USA PATRIOT Act, which directs his office to undertake a series of actions related to complaints of civil rights or civil liberties violations allegedly committed by DOJ employees. In his testimony, Mr. Fine noted that, with the exception of the Brandon Mayfield case, none of the allegations received by his office alleging misconduct by a Department employee related to use of a provision of Patriot Act. That is a significant finding.

### Conclusion

Mr. Chairman, I'd like to say a final word about congressional oversight and my concern that Congress, while reauthorizing the USA PATRIOT Act, may seek to include new sunsets. In just the last few weeks, the Attorney General and I have met with dozens of Members of Congress to discuss these important tools. In addition, the Attorney General has appeared three times to testify. Moreover, 32 Department of Justice witnesses have appeared at 17 Congressional hearings which have explored in depth the various tools contained in the USA PATRIOT Act. All of this activity is because Congress is rightly engaging in its critical role to conduct appropriate oversight. But sunsets are not required to conduct oversight. Congress maintains its authority and responsibility to conduct oversight, to ask questions, to demand answers, even without sunsets. My concern is that sunsets on these important tools might inhibit the culture of information sharing that we are trying to foster. Rather than encouraging and empowering our agents and prosecutors to rely upon these new tools, we send a message that a particular provision may only be temporary and chill development of the culture of information sharing. As long as congressional oversight remains robust, which I am convinced it will, there is no need for sunsets.

Mr. Chairman, again, thank you for the opportunity to appear before you today and thanks to you and all your colleagues for providing us with the important tools of the USA PATRIOT Act. I would now be happy to answer any questions.

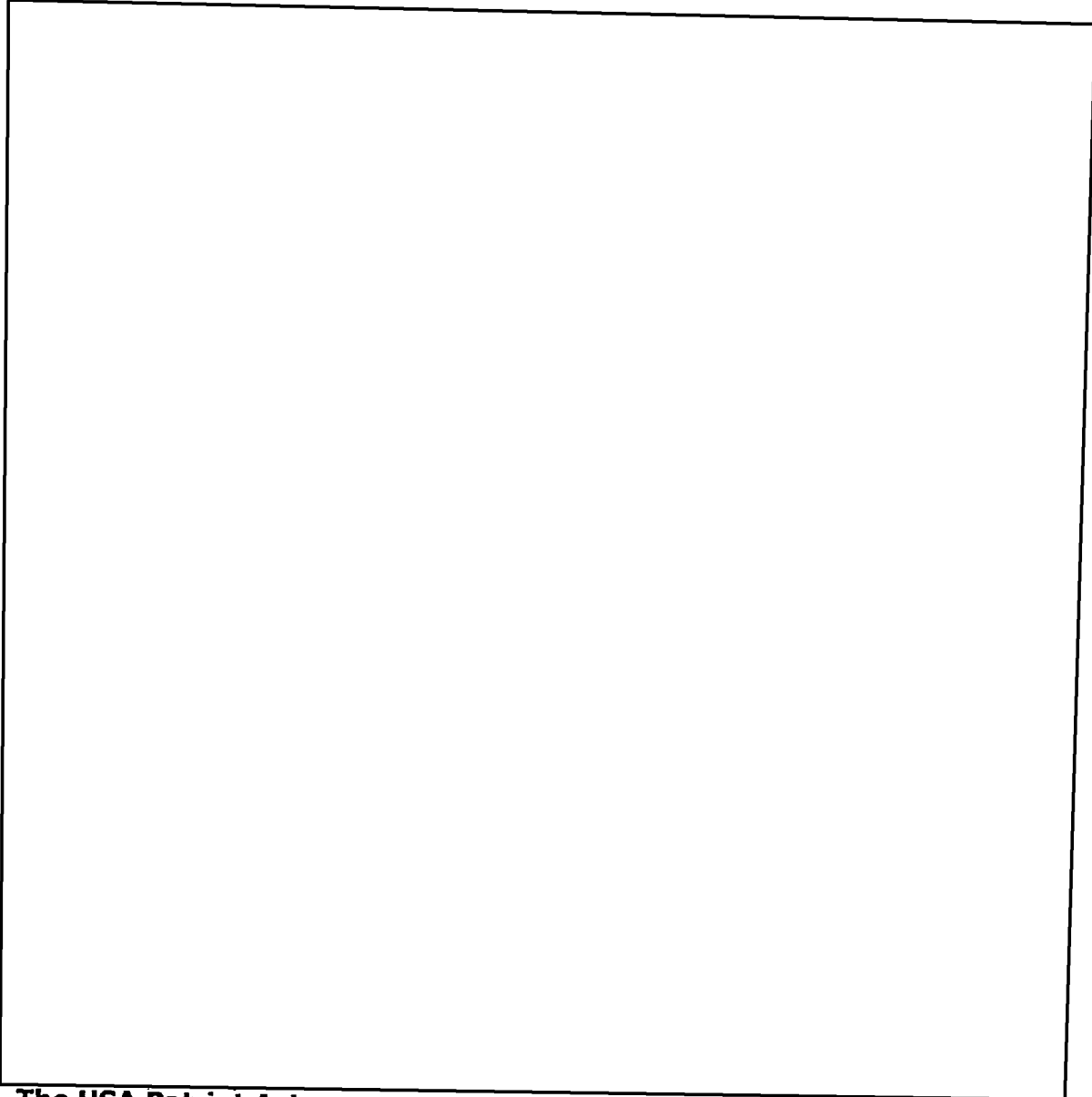


Office of Public Affairs

## Q&As for Press Availability

Outside the Scope

*September 21, 2005*



**The USA Patriot Act .....61**



## The USA Patriot Act

**Issue:** There has been widespread media interest related to the USA PATRIOT Act, particularly the debate over 16 provisions up for renewal by Congress set to expire at the end of this year. Areas of particular interest include administrative subpoenas and library/book store records.

**Status:** On 07/21/2005, the House passed Rep. James Sensenbrenner's bill (257 to 171) to extend the Patriot Act search provisions. The House bill includes a requirement that the FBI director approve any request for records from a library or bookstore. It would make 14 of the expiring provisions permanent and extend two others -- pertaining to records seizures and roving wiretaps -- for a decade." The *AP* (7/22, Johnson) and *Reuters* (7/22, Elsner) also note the amendment requiring the Director's personal approval for library and bookstore records.

Meanwhile, the Senate Judiciary Committee approved the Specter-Feinstein bill that, as the *Washington Post* (7/22, A12, Eggen) noted, "would allow people to challenge warrants approved by a secret Foreign Intelligence Surveillance Court and would require that subjects of secret sea." *USA Today* (7/22, Locy) reported that the Senate bill also eliminates "a gag order provision that prohibits any business from speaking about an FBI request for information." USA notes, "The *New York Times* (7/22, Lichtblau) notes the House bill "would make permanent 14 of the 16 provisions in the law that are set to expire at the end of this year. The remaining two provisions -- giving the government the power to demand business and library records and to conduct roving wiretaps - would have to be reconsidered by Congress in 10 years.

On 07/24/2005, the *New York Times* (Lichtblau) reported on opposition to a Patriot Act amendment that would force the government to disclose its use of data-mining techniques in tracking suspects in terrorism cases." The House voted to "include a little-noticed provision that would require the Justice Department to report to Congress annually on government-wide efforts to develop and use data-mining technology to track intelligence patterns."

### **Q&As:**

Outside the Scope





**\* IMPACT ON LIBRARY AND BOOK STORE RECORDS**

On 05/17/05, in a *USA Today* Op/Ed piece, the Director of the Library District in Whatcom County, WA, discussed how her experience with the FBI via its authority to obtain library and bookstore records has shaped her view on the USA Patriot Act. She specifically cites an incident in June 2004 when an FBI Agent requested a list of the people who borrowed a biography of Usama Bin Laden. The author states this experience has taught her and her fellow library trustees... "How easily the FBI could have discovered the names of the borrowers, how readily this could happen in any library in the USA. It also drove home for us the dangers that the USA Patriot Act posed to reader privacy." The author notes that... "in the

current debate over extending or amending the Patriot Act, one of the key questions is whether a library or any other institution can seek an independent review of an order. Even the attorney general conceded in a recent oversight hearing that this is a problem with the law as written."

***Does the Patriot Act include any specific language to library (or bookstore) records?***

1. The Patriot Act is not directed at library or bookstore records. Section 215 does permit the FISA Court to issue an order to produce "tangible things," including business and other records, in support of a foreign intelligence or international terrorism investigation. It also prohibits notice to the customer whose records are ordered to be produced.
  - a. The section could conceivably be used to obtain records from a library or bookstore but only if such records were relevant to an FBI foreign intelligence or international terrorism investigation.
  - b. This authority cannot and will not be used to monitor the reading habits of library patrons or even those of certain groups or members of certain organizations. If used, it would be used in a specific case for a specific individual and based on a valid investigative reason. For example, if the FBI received credible information that a suspected terrorist was believed to have checked out some books from a specific library on building a bomb or dispersing a chemical or biological substance, the FISA Court may issue an order to that library to produce the specific records within a known time frame concerning a named patron.
2. If Section 215 were used to obtain patron records from a library or bookstore, its impact would be case specific, isolated and, in the end, inconsequential to the day-to-day business of the Nation's libraries and bookstores



Office of Public Affairs

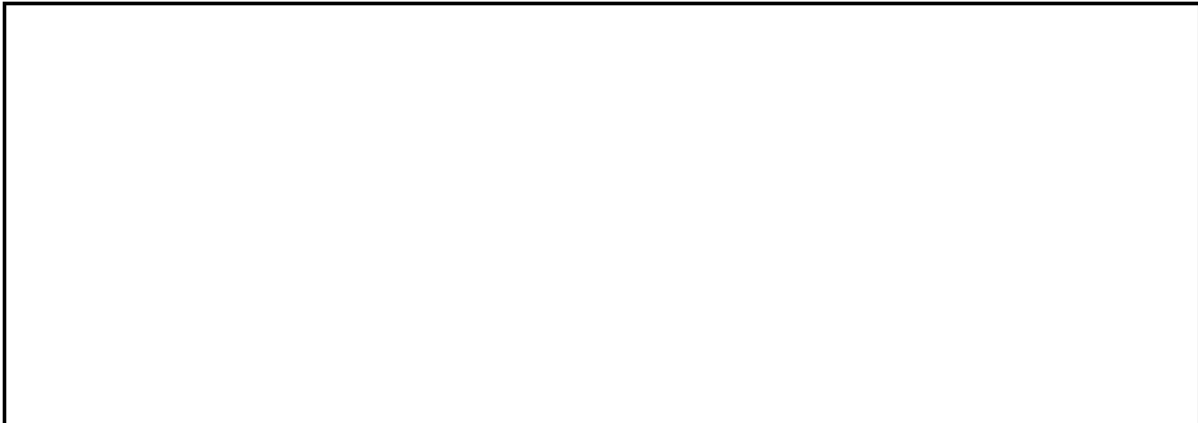
**Director Robert S. Mueller III  
Federal Bureau of Investigation**

**Anti-Defamation League  
New York, NY**

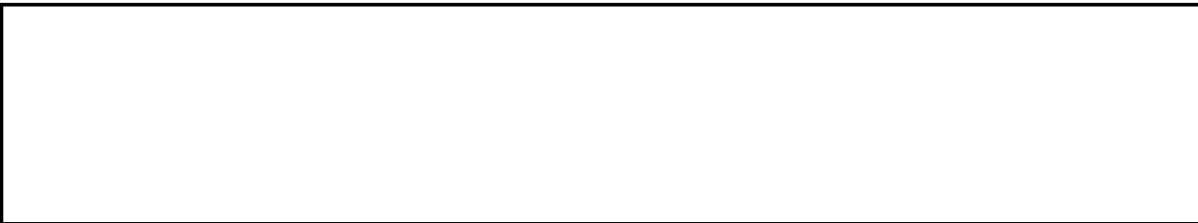
*November 3, 2005*

**Q&As**

Outside the Scope



**The USA Patriot Act .....17**



S. HRG. 109-168

# OVERSIGHT OF THE USA PATRIOT ACT

---

---

## HEARINGS

BEFORE THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 5, AND MAY 10, 2005

Serial No. J-109-10

Printed for the use of the Committee on the Judiciary





**OVERSIGHT OF THE USA PATRIOT ACT**

S. HRG. 109-168

**OVERSIGHT OF THE USA PATRIOT ACT**

---

---

**HEARINGS**  
BEFORE THE  
**COMMITTEE ON THE JUDICIARY**  
**UNITED STATES SENATE**  
ONE HUNDRED NINTH CONGRESS  
FIRST SESSION

APRIL 5, AND MAY 10, 2005

**Serial No. J-109-10**

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

24-293 PDF

WASHINGTON : 2005

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

EFF Section 215-607

· COMMITTEE ON THE JUDICIARY

ARLEN SPECTER, Pennsylvania, *Chairman*

ORRIN G. HATCH, Utah	PATRICK J. LEAHY, Vermont
CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
JON KYL, Arizona	JOSEPH R. BIDEN, JR., Delaware
MIKE DEWINE, Ohio	HERBERT KOHL, Wisconsin
JEFF SESSIONS, Alabama	DIANNE FEINSTEIN, California
LINDSEY O. GRAHAM, South Carolina	RUSSELL D. FEINGOLD, Wisconsin
JOHN CORNYN, Texas	CHARLES E. SCHUMER, New York
SAM BROWNBACK, Kansas	RICHARD J. DURBIN, Illinois
TOM COBURN, Oklahoma	

DAVID BROG, *Staff Director*

MICHAEL O'NEILL, *Chief Counsel*

BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

## CONTENTS

TUESDAY, APRIL 5, 2005

### STATEMENTS OF COMMITTEE MEMBERS

	Page
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois .....	37
Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin, prepared statement .....	247
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa, prepared statement .....	280
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah .....	15
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont .....	3
prepared statement .....	283
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania .....	1

### WITNESSES

Gonzales, Alberto R., Attorney General, Department of Justice, Washington, D.C. ....	5
Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C. ....	9

### QUESTIONS AND ANSWERS

Responses of Alberto R. Gonzales to questions submitted by Senators Specter, Kennedy, Durbin, Grassley, Biden, Feingold, Kyl, and Leahy (June 29, 2005) .....	59
Responses of Alberto R. Gonzales to questions submitted by Senators Specter, Kennedy, Biden, Feingold, Kyl, and Leahy (October 20, 2005) .....	114
Responses of Robert S. Mueller III to questions submitted by Senators Grassley, Kyl, Leahy and Feingold .....	192

### SUBMISSIONS FOR THE RECORD

Gonzales, Alberto R., Attorney General, Department of Justice, Washington, D.C., prepared statement .....	249
Moschella, William E., Assistant Attorney General: .....	
report on applications to Foreign Intelligence Surveillance Court, April 1, 2005 .....	287
report on translation services, April 1, 2005 .....	289
Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement .....	304

TUESDAY, MAY 10, 2005

### STATEMENTS OF COMMITTEE MEMBERS

	Page
Biden, Hon. Joseph R., Jr., A U.S. Senator from the State of Delaware .....	331
Cornyn, Hon. John, a U.S. Senator from the State of Texas .....	321
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois .....	322
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont .....	316
prepared statement .....	441
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania .....	315

(III)

IV

WITNESSES

	Page
Barr, Bob, former Representative in Congress from the State of Georgia .....	333
Cole, David, Professor of Law, Georgetown University Law Center, Wash- ington, D.C. ....	334
Collins, Daniel P., Munger, Tolles and Olsen, LLP, Los Angeles, California .....	336
Craig, Hon. Larry E., a U.S. Senator from the State of Idaho .....	318
Dempsey, James X., Executive Director, Center for Democracy & Technology, Washington, D.C. ....	338
McCarthy, Andrew C., Senior Fellow, Foundation for the Defense of Democ- racies, Washington, D.C. ....	340
Spaulding, Suzanne E., Managing Director, The Harbour Group, LLC, Wash- ington, D.C. ....	342

QUESTIONS AND ANSWERS

Response of Dan Collins to a question submitted by Senator Biden .....	361
Response of Suzanne E. Spaulding to a question submitted by Senator Leahy .....	363

SUBMISSIONS FOR THE RECORD

American Booksellers Association, American Library Association, Association of American Publishers, PEN American Center, Washington, D.C., joint letter .....	365
American Jewish Committee, Richard T. Foltin, Legislative Director and Counsel, Washington, D.C., letter .....	367
Ashcroft, John, former Attorney General, Department of Justice, Washington, D.C., letter .....	369
Barr, Bob, former Representative of Congress from the State of Georgia, prepared statement and letter .....	378
Cole, David, Professor of Law, Georgetown University Law Center, Wash- ington, D.C., prepared statement .....	389
Collins, Daniel P., Munger, Tolles and Olsen, LLP, Los Angeles, California, prepared statement .....	406
Dempsey, James X., Executive Director, Center for Democracy & Technology, Washington, D.C., prepared statement .....	426
League of Women Voters, Kay J. Maxwell, President, Washington, D.C., letter .....	440
McCarthy, Andrew C., Senior Fellow, Foundation for the Defense of Democ- racies, Washington, D.C., prepared statement .....	444
Moschella, William E., Assistant Attorney General, Department of Justice, Washington, D.C.: letter, May 3, 2005 .....	479
letter, May 6, 2005 .....	486
Salazar, Hon. Ken, a U.S. Senator from the State of Colorado, prepared statement .....	489
Senate Bill of Rights Caucus, statement of principles and attachment .....	491
Spaulding, Suzanne E., Managing Director, The Harbour Group, LLC, Wash- ington, D.C., prepared statement .....	493

## OVERSIGHT OF THE USA PATRIOT ACT

TUESDAY, APRIL 5, 2005

UNITED STATES SENATE,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Committee met, pursuant to notice, at 9:30 a.m., in Room SD-216, Hart Senate Office Building, Hon. Arlen Specter, Chairman of the Committee, presiding.

Present: Senators Specter, Hatch, Kyl, Sessions, Cornyn, Coburn, Leahy, Kennedy, Feinstein, Feingold, and Schumer.

### OPENING STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Chairman SPECTER. Ladies and gentlemen, the hour of 9:30 having arrived, the Senate Judiciary Committee will not proceed to this hearing on the PATRIOT Act, and the Committee welcomes Attorney General Alberto Gonzales for his first appearance before this Committee after his confirmation and, similarly, we welcome FBI Director Robert Mueller to take up this very important subject.

I have had a considerable number of comments about my health, some on the way walking in this morning, so just a brief comment. I have had about a third of the treatments. I am doing fine. The doctor predicts a full recovery. I have been on the job. In the last 2 weeks during the recess, I could not travel a road and spent most of the time here in Washington on the job. The most noticeable effect has been the involuntary new hairstyling.

Senator LEAHY. I think it looks great.

Chairman SPECTER. Well, Patrick, we are practically tied at this point.

[Laughter.]

Chairman SPECTER. But I am assured that within a few months I will be back to a head of hair comparable to Attorney General Gonzales, maybe not quite comparable, but close.

The hearing on the PATRIOT Act poses very fundamental questions of security for our country, with appropriate concern for constitutional and civil rights. There is no doubt that the fundamental responsibility of Government is to protect its citizens, and in the United States, with our deep tradition for civil rights and constitutional law, that concern for security has to be balanced by new regard for civil rights.

The report, which was just issued last week by the Commission on Intelligence Capabilities of the United States regarding weapons of mass destruction, contains some very disquieting conclusions

which bear directly upon the efficacy of the PATRIOT Act and our overall efforts as security.

Without going into the conclusions in any depth at this time, a couple point up the basic concern where the Commission reported that the clashes between the various intelligence agencies, concentrating specifically on the CIA and FBI, exist not only in regards to which agency gets credit for intelligence reports, but also in the field where lives are at stake. The Commission went on further to say, "The failure of the CIA and FBI to cooperate and share information adequately on cases could potentially create a gap in coverage of these threats like the one on September 11th, which the attack plotters were able to exploit."

The Committee will be engaging in comprehensive oversight reality on the model that the Committee used on Ruby Ridge about a decade ago. A team has already met with Director Mueller on the issue of coordination, set up where I contacted him, personally, and we met with representatives of our staffs on February the 1st. The report which Director Mueller gave was significantly more optimistic with respect to the coordination than as has been the report of the Commission last week. That is something that we will want to consider during the course of these hearings but, as noted, the principal focus of the hearings is on the PATRIOT Act itself.

In my view, there are very, very important provisions in the PATRIOT Act which need to be reauthorized, not all perhaps, but some very important provisions. The wall separating the Foreign Intelligence Surveillance Act is down and has been very, very useful in law enforcement so that evidence obtained pursuant to the Foreign Intelligence Surveillance Act warrant can be used in a criminal proceeding. The provisions on nationwide search warrants are certainly necessary. The material support for terrorist prohibition is a very important provision.

There have been questions raised by both the right and the left on the political spectrum about some of the other provisions, as we all know, with respect to the authority to seize tangible things. The illustration of that has been the library books, so to speak, and we will hear from the Attorney General and the Director on this subject.

The question arises, in my mind, as to whether the traditional standards for probable cause ought not to be used in obtaining materials of that sort, a concern that I expressed to Attorney General Gonzales during his confirmation hearings and I have expressed also to Director Mueller. The issues of the so-called sneak-and-peek provisions, where there are five exceptions, and one of the exceptions is so broad that it could be a coverall to not have a limit of time as to when the subject of the sneak-and-peek is informed. That is something which we will take a look at.

The roving wiretaps provision has also been subject to certain challenges to the identity of the person, whether a description is sufficient and how many technical means can be used to obtain.

Those are all issues which we will look into during the course of this hearing.

We have asked the Attorney General and Director to limit their opening remarks to 10 minutes, with their full statements made a part of the record. We will work through until 1 o'clock or a con-

venient break point about that time, and the Attorney General and the Director have already been asked to be available in the afternoon because I think we will have a large attendance at this session with questions. We will have 7-minute rounds of questions. I am right up to 7 minutes now, and I want to yield, at this point, to my distinguished ranking member, Senator Leahy.

**STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR  
FROM THE STATE OF VERMONT**

Senator LEAHY. Thank you very much, Mr. Chairman. I do feel this is an extremely important meeting, and it is good to have oversight. I was delighted, also, to hear your comments about going back to the kind of oversight we did with Ruby Ridge. I agree with you that that was an example of how oversight can and should be done, and we should go back to that.

On a September morning, as we all know, three-and-a-half years ago nearly 3,000 lives were lost on American soil. Our lives, our lives as Americans, changed instantly. In the aftermath of the 9/11 attacks Congress moved quickly—some have said too quickly—to give Federal authority substantial new powers to investigate and prosecute terrorism. The USA PATRIOT Act was signed into law just 6 weeks later.

Some of us sitting here today contributed to the PATRIOT Act. We worked together in a bipartisan manner, and with common resolve to craft a bill that we hoped would make us safer as a Nation. Freedom and security are always in tension in our society, but we tried our best to strike the right balance. Now it is time to return to this discussion to assess what aspects we got right and what modifications need to be made.

I negotiated many of the provisions of the PATRIOT Act and am gratified to have been able to add several checks and balances that were not in the initial proposal. The White House broke its word on some agreements that we had mutually reached to strike a better balance on some of the PATRIOT Act's provisions. It is also true that additional checks and balances that I and others sought, had the White House agreed to them, would have yielded the same benefits to our law enforcement efforts, but with greater accountability. In the final negotiating session, former House Majority Leader Dick Armey and I joined together to insist that we add a sunset for certain governmental powers that have great potential to affect the civil liberties of the American people. That is why we are here today because that sunset provision ensured that we would revisit the PATRIOT Act and shine some sunlight on how it has been implemented.

Before we rush to renew any controversial powers created by the PATRIOT Act, we need to understand how these powers have been used and whether they have been effective. A few weeks ago, we celebrated the first national Sunshine Week with a hearing on open Government and bipartisan calls for accountability. We should do the same in our oversight.

We should bear in mind the 9/11 Commission's counsel about the PATRIOT Act. They wrote, "The burden of proof for retaining a particular governmental power should be on the Executive to explain, A, that the power actually materially enhances security, and,



B, that there is adequate supervision of the Executive's use of the powers to ensure protection of civil liberties."

We are in a new Congress with a new Chairman of this Committee. Chairman Specter has a distinguished record as a steadfast advocate and practitioner of meaningful oversight—of meaningful oversight. We have before us a new Attorney General who has pledged to work with us on a number of issues, including the PATRIOT Act. The American people deserve to be represented by a Congress that takes its oversight responsibilities seriously. The breakdown of cooperation following the passage of the PATRIOT Act has fostered distrust. We can change that by working together to achieve the right balance in our Antiterrorism Act by allowing the appropriate amount of sunshine to light what we are doing.

We have heard over and over again there have been no abuses as a result of the PATRIOT Act, but it has been difficult, if not impossible, to verify that claim when some of the most controversial surveillance powers in the act operated under a cloak of secrecy. We know the Government is using its surveillance powers under the Foreign Intelligence Surveillance Act more than ever, but everything else about FISA is secret. This difficulty of assessing the impact on civil liberties has been exacerbated greatly by the administration's obstruction of legitimate oversight.

Now, whether or not there have been abuses under the PATRIOT Act, the unchecked growth of secret surveillance powers and technology, with no real oversight by the Congress to the courts, has resulted in clear abuses by the executive branch. We have seen secret arrests and secret hearings of hundreds of people for the first time in U.S. history; detentions without charges and denial of access to counsel; misapplication of the material witness statute as a sort of general prevention detention law; discriminatory targeting of Arabs and Muslims; selective enforcement—selective enforcement—of the immigration laws; and the documented mistreatment of aliens held on immigration charges.

These abuses harm our national security as well as civil liberties. They serve as recruiting posters for terrorists, intimidate American communities from cooperating with law enforcement agencies, and when they misuse limited antiterrorism resources, they make it more likely real terrorists are going to escape detection.

Beyond this, the administration has used brutal and degrading interrogation techniques against detainees in Afghanistan, Iraq, and Guantanamo Bay. Those run counter to past American military traditions. Information about these disgraceful acts continue to trickle out in large part only because of a persistent press and the use of FOIA not by the oversight this Congress should do.

In yet another example of abuse, recent press reports provide disturbing details about how the administration embraced the use of extraordinary rendition after the 9/11 attacks. Several press reports detail the CIA's use of jets to secretly transfer detainees to places around the world where they were going to be tortured.

In defending the administration's rendition policy, the President said, in his March 17 press conference, that "we seek assurances that nobody will be tortured when we render a person back to their home country." That statement came only 10 days after Attorney General Gonzales acknowledged that we cannot fully control what

happens to detainees transferred to other Nations. He added that he does not know whether these countries have always complied with their promises.

There are always going to be scandals and tragedies in a Nation's history. What makes America special is that we do not hide from our mistakes; we investigate them, we learn from them; and we make sure they do not happen again. When necessary, we change our laws to reflect the lessons we have learned. The spirit of openness and accountability are what bring us here today to reconsider portions of the PATRIOT Act.

Mr. Chairman, I applaud you for doing this. The kind of oversight that you have is similar to what you did in Ruby Ridge, and we are going to be doing far, far better for the country, for the Committee, and for the Senate.

Chairman SPECTER. Thank you very much, Senator Leahy.

Attorney General Gonzales and Director Mueller, would you rise, please.

Do each of you solemnly swear that the testimony you will present before the Senate Judiciary Committee will be the truth, the whole truth and nothing but the truth so help you God?

Attorney General GONZALES. I do.

Director MUELLER. I do.

Chairman SPECTER. Attorney General Gonzales, we again welcome you here for the first of the oversight hearings. We note some of your recent comments showing some willingness to consider some modifications. They have been described in the media as technical, but we welcome that approach, and we look forward to your testimony.

The floor is yours.

**STATEMENT OF ALBERTO R. GONZALES, ATTORNEY GENERAL,  
DEPARTMENT OF JUSTICE, WASHINGTON, D.C.**

Attorney General GONZALES. Thank you, Mr. Chairman. Chairman Specter, Senator Leahy and members of the Committee, I am pleased to be here with Director Mueller to discuss an issue relating to the security of the American people.

Following the attacks of September 11th, 2001, the administration and Congress did come together to prevent such a tragedy from happening again. One result of our collaboration was the USA PATRIOT Act, which was passed by Congress with overwhelming bipartisan support. Since then, the Act has been integral to the Government's prosecution of the war on terrorism. Thanks, in part, to the act, we have dismantled terrorist cells, disrupted terrorist plots and captured terrorists before they could strike.

Many of the most important authorities in the Act are scheduled to expire on December 31, 2005. It is important that these authorities remain available, in my judgment. Al Qaeda and other terrorist groups still pose a grave threat to the security of the American people, and now is not the time to relinquish some of our most effective tools in this fight.

As Congress considers whether to renew these provisions, I am open to suggestions for clarifying and strengthening the act. I look forward to meeting with those, both inside and outside of Congress, who have expressed concerns about the act, but let me be clear

that I will not support any proposal that would undermine our ability to combat terrorism effectively.

All of us have the same objective, ensuring the security of the American people, while preserving our civil liberties. I, therefore, hope that we will consider reauthorization in a calm and thoughtful manner. Our dialogue should be based on facts rather than exaggeration. Because I believe that this discussion must be conducted in an open and honest fashion, I will begin my testimony today by presenting this Committee with new information recently declassified about the use of certain PATRIOT Act provisions.

Of the 16 provisions scheduled to sunset, some members of this Committee had raised the most concern about Sections 206 and 215. Section 215 granted national security investigators authority to seek a court order requiring the production of records relevant to their investigation. Just as prosecutors use grand jury subpoenas as the building blocks of criminal investigations, investigators in international terrorism and espionage cases must have the ability, with appropriate safeguards, to request production of evidence that can be essential to the success of an intelligence investigation.

To be clear, a Section 215 order, like a subpoena, does not authorize Government investigators to enter anyone's home or search anyone's property. It is merely a request for information. A Federal judge must approve every request for records under Section 215, and the FISA Court has granted the Department's request for a 215 order 35 times, as of March 30, 2005.

Although prosecutors have long been able to obtain library records in connection with a criminal investigation, I recognize that Section 215 may be the act's most controversial provision principally because of fears concerning the theoretical use of the provision to obtain library records. However, I can report the Department has not sought a Section 215 order to obtain library or bookstore records, medical records or gun sale records; rather, the provision, to date, has been used only to obtain driver's license records, public accommodation records, apartment leasing records, credit card records and subscriber information such as names and addresses for telephone numbers captured through court-authorized pen register devices.

Going forward, the Department anticipates that our 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 just as such information is routinely obtained in criminal investigations.

Although some of the concerns expressed about Section 215 have been based on inaccurate fears about its use, other criticisms have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a Section 215 order may consult with his attorney and may challenge that order in Court. The Department has also stated that the Government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevant standard that applies to grand jury subpoenas in criminal cases.

The text of Section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points. We cannot, however, support elevating the relevance standard under Section 215 to probable cause. According to our lawyers and agents, raising the standard would render Section 215 a dead letter. As we all know, probable cause is a standard that law enforcement must meet to justify an arrest. It should not be applied to preliminary investigative tools such as grand jury subpoenas or Section 215 orders which are used to determine whether more intrusive investigative techniques requiring probable cause, such as electronic surveillance, are justified.

Section 206, also, provides terrorism investigators with an authority long possessed by criminal investigators. In 1986, Congress authorized the use of multi-point or roving wiretaps in criminal investigations. Before the PATRIOT Act, however, these orders were not available for national security investigations under FISA. Therefore, when international terrorists or spies switch telephones, investigators had to return to the FISA Court for a new surveillance order and risk missing key conversations. In a post-9/11 world, we cannot take that risk.

Section 206 fixed this problem by authorizing multi-point surveillance of international terrorists or a spy when a judge finds that the target may take action to thwart surveillance. As of March 30th, this provision had been used 49 times and has been effective in monitoring international terrorists and spies.

Another important FISA-related PATRIOT Act provision is Section 207. Prior to the act, the Justice Department invested considerable time returning to court to renew existing orders granted by the FISA Court. Section 207 substantially reduced this investment of time by increasing the maximum time duration for FISA electronic surveillance and physical search orders.

The Department estimates that Section 207 has saved nearly 60,000 attorney hours. In other words, it has saved 30 lawyers a year's work, and this estimate does not account for time saved by FBI agents, administrative staff and the Judiciary. Department personnel were able to spend that time pursuing other investigations and oversight matters.

Given Section 207's success, I am, today, proposing additional amendments to increase the efficiency of the FISA process, copies of which will be presented to this Committee today. Had these proposals been included in the PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission, which said that the amendments would allow the Department both to focus their attention where it is most needed and to maintain the current level of oversight paid to cases implicating the civil liberties of Americans.

Finally, I would like to touch on another provision that has generated significant discussion—Section 213—which is not scheduled to sunset. It established a nationwide standard for issuing delayed-notice search warrants which have been used by law enforcement in criminal investigations and approved by courts for decades, as we all know.

Under Section 213, law enforcement must always, always provide notice to a person whose property is searched. A judge may allow that notice to be temporarily delayed in a few circumstances, but that person will always receive notification. The Department uses this tool only where necessary. For instance, from enactment of the PATRIOT Act through January 31, 2005, the Department used Section 213 to request approximately 155 delayed-notice search warrants which have been issued in terrorism, drug, murder and other criminal investigations. We estimate that this number represents less than one-fifth of 1 percent of all search warrants obtained by the Department during this time. In other words, in more than 499 of 500 cases, the Department provides immediate notice of a search. In appropriate cases, however, delayed-notice search warrants are necessary because if terrorists or other criminals are prematurely tipped off that they are under investigation, they may destroy evidence, harm witnesses or flee prosecution.

I hope that the information I have presented will demystify these essential national security tools, eliminate some of the confusion surrounding their use and enrich the debate about the Department's counterterrorism efforts. The tools I have discussed today are critical in my judgment to our Nation's success in the war against terrorism. I am, therefore, committed to providing the information that this Committee and the American public need to thoroughly evaluate the PATRIOT Act. The Act has a proven record of success in protecting the security of the American people, and we cannot afford to allow its most important provisions to sunset.

I look forward to working with the Committee closely in the weeks ahead, listening to your concerns and joining together again to protect the security of the American people. Thank you, Mr. Chairman.

[The prepared statement of Attorney General Gonzales appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Attorney General Gonzales.

Senator LEAHY. Mr. Chairman?

Chairman SPECTER. Senator Leahy?

Senator LEAHY. I just would ask consent that the Attorney General has submitted testimony, which we all received, and testimony actually delivered here today both be in the record because there are some substantial differences.

Senator LEAHY. Without objection, the written testimony submitted will be made a part of the record. I think I noted that earlier, but, in any event, they will be made a part of the record.

We now turn to the Director of the FBI. We welcome you, again, Director Mueller. Thank you for your courtesies of the recent meeting which you and I had with our respective staffs, and we will be pursuing that, among other matters.

Now, we look forward to your testimony.

**STATEMENT OF ROBERT S. MUELLER III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.**

Director MUELLER. Thank you, and good morning, Mr. Chairman. Good morning, Senator Leahy and members of the Committee. I am pleased to be here today with the Attorney General to talk about the PATRIOT Act and how it has assisted the FBI with its efforts on the war on terror.

The PATRIOT Act has, indeed, changed the way that we in the FBI operate, and it has assisted us, in many ways, in our counterterrorism successes. My formal statement was submitted for the record, and it focuses primarily on the 16 provisions that are scheduled to sunset at the end of this year. While I firmly believe it is very important to our national security that these provisions be renewed, I want to emphasize this morning the importance of the information-sharing provisions to the war on terror.

Mr. Chairman, the information-sharing provisions are consistently identified by FBI field offices as the most important provisions in the PATRIOT Act. The ability to share crucial information has significantly altered the landscape for conducting terrorism investigations, allowing for a more coordinated and effective approach. Specifically, our field offices note that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that, first of all, enables us to be more effective and responsive in our investigative efforts, improves the utilization of our resources, allows for follow-up investigations by other agencies—for instance, when the subject of the investigation leaves the United States—and it, also, helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the PATRIOT Act provided for some exchange of information, the law was complex and, as a result, agents often erred on the side of caution and refrained from sharing information. The PATRIOT Act's information-sharing provisions, Sections 203 and 218, eliminated that hesitation and allows agents to more openly work with other Government entities, resulting in a much stronger team approach. This approach is necessary in order to effectively prevent and detect the complex web of terrorist activity.

FBI field offices report enhanced liaison with State, local, tribal and, as important, other Federal agencies, including the intelligence agencies across the country. Our legal attache offices overseas report improved relationships with other intelligence agencies operating overseas.

Prior to the PATRIOT Act, Federal law was interpreted to prohibit criminal investigators from disclosing criminal wiretap or grand jury information to counterparts working on intelligence investigations.

Sections 203(a) and (b) of the PATRIOT Act eliminated these barriers to information sharing, allowing for routine sharing of information derived from these important criminal tools.

Section 203(d) ensures that information developed through law enforcement methods other than grand jury testimony or criminal wiretaps can also be shared with intelligence partners at the Federal, State and local levels, as well as with our partners overseas.

Section 218 of the PATRIOT Act was the first step in dismantling the wall between criminal and intelligence investigators. It eliminates the primary purpose requirement under FISA and replaces it with a significant purpose test. FBI agents working on intelligence and counterintelligence matters now have greater latitude to consult criminal investigators or prosecutors without putting their investigations at risk.

Prosecutors are now involved at the earliest stages of international terrorism investigations, and prosecutors are often co-located with the Joint Terrorism Task Forces and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks.

Mr. Chairman, if these information-sharing provisions are allowed to sunset, the element of uncertainty and confusion that existed in the past will be reintroduced. Agents will again hesitate and spend precious time seeking clarification of complicated information-sharing restrictions. This hesitation will lead to less teamwork, less efficiency and, ultimately, loss of effectiveness in the war on terror.

Experience has taught the FBI that there are no clear dividing lines that distinguish criminal, terrorist and foreign intelligence activity. Criminal, terrorist and foreign intelligence organizations and their activities are often interrelated or interdependent. FBI files contain many examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence investigations was essential to our ability to protect the United States from terrorist or intelligence activity and criminal activity.

For example, the FBI investigated a group of Pakistan-based individuals who were participating in arms trafficking, the production and distribution of multiton quantities of hashish and heroin and participate in the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by al Qaeda in Afghanistan. The operation, thanks to the ability to share information, resulted in the arrest, indictment and subsequent extradition of the subjects from Hong Kong to San Diego to face charges of providing material support to al Qaeda, as well as charges relating to their drug activities.

In yet another example in the aftermath of September 11th, a reliable intelligence source identified a naturalized United States citizen from the Middle East as being a leader among a group of Islamic extremists operating in the United States. The subject's extremist views, affiliations with other terrorist subjects and heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities.

Early in the criminal investigation, it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. A close interaction between the criminal and intelligence cases was critical to the successful arrest of the subject before he was able to leave the country, and it ultimately resulted in his guilty plea to criminal charges.

The increased coordination and information sharing between intelligence and law enforcement agents facilitated by the PATRIOT

Act has allowed the FBI to approach cases such as these as a single integrated investigation that allows us to see the full picture not separate pieces of a criminal case, separate pieces of an intelligence case, separate pieces of information. It allows us to work together to successfully bring together various pieces of information regardless of whether it is in the field of counterintelligence, terrorism or criminal and enables us to depend on that free flow of information between respective investigations, investigators, and analysts to successfully perform our responsibilities.

Mr. Chairman, critics of the PATRIOT Act's information-sharing provisions have suggested that they lack sufficient safeguards or that they can be used to circumvent constitutional safeguards by conducting a search or wiretap for the purpose of investigating a crime without demonstrating probable cause that a crime has been committed. These concerns ignore the considerable safeguards and limitations that are firmly in place.

With respect to changes in the wiretap statute, Section 203(b) only allows for the sharing of a certain limited class of information gathered under Title III, such as information relating to a serious national security matter. In addition, the Title III statute imposes substantial burdens on law enforcement and judicial approval prior to the initiation of the wiretap. Section 203(b) does not reduce these requirements. It simply permits the appropriate sharing of information after it is collected under court order.

Mr. Chairman and members of the Committee, the provisions of the PATRIOT Act that I have discussed today are crucial to our present and future success in the global war on terrorism. By responsibly using the statute provided by Congress, the FBI has made substantial progress in our ability to proactively investigate, and prevent terrorism and to protect lives, while, at the same time and as important, protecting civil liberties.

In renewing these provisions scheduled to sunset at the end of this year, Congress will ensure that the FBI will continue to have the tools we need to combat the very real threat to America posed by terrorists and their supporters.

Mr. Chairman, thank you, again, for the opportunity to appear before you today, and I, too, am happy to answer any questions you might have.

[The prepared statement of Director Mueller appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Director Mueller.

We will now proceed with the 7-minute rounds in order of arrival, which is the custom of the Committee.

Attorney General Gonzales, I am pleased to see some of the modifications which you have suggested would be acceptable to the Department of Justice with respect to the recipient may consult an attorney, the recipient may challenge in court not only documents relevant to national security investigations would be involved.

I note that on the information provided by the Department of Justice there has not been a request under the "tangible things" category for library or medical records. That has been an area of substantial concern to some. Would you see any problem on specifically excluding, in a reauthorization of the PATRIOT Act, authority to obtain a library or medical records?



Attorney General GONZALES. Mr. Chairman, let me try to reassure the Committee and the American people that the Department has no interest in rummaging through the library records or the medical records of Americans. That is not something that we have an interest in. We do have—

Chairman SPECTER. Does that mean you would agree to excluding them?

Attorney General GONZALES. We do have an interest, however, in records that may help us capture terrorists, and there may be an occasion where having the tools of 215 to access this kind of information may be very helpful to the Department in dealing with a terrorist threat.

The fact that this authority has not been used for these kinds of records means that the Department, in my judgment, has acted judiciously. It should not be held against us that we have exercised, in my judgment, restraint. It is comparable to a police officer who carries a gun for 15 years and never draws it. Does that mean that for the next 5 years he should not have that weapon because he has never used it?

Chairman SPECTER. Attorney General Gonzales, I do not think your analogy is apt, but if you want to retain those records as your position, I understand, and let me move on.

The staff of the Judiciary Committee was briefed by the Department of Justice last month, and we were advised that it takes an average of 71 days to obtain a warrant under the Foreign Intelligence Surveillance Act. Does that sound right to you?

Attorney General GONZALES. Sir, I do not know whether or not that is an accurate number. Perhaps Director Mueller might have more information about that.

Chairman SPECTER. Would you check on that?

Attorney General GONZALES. I will check on that.

Chairman SPECTER. Because if it is true, and I note Director Mueller's forehead furrowing a bit on that. It would certainly be very stale on the kind of information that a law enforcement officer would need. We have seen on oversight from this Committee before, going back to Wen Ho Lee, enormous problems in the Department of Justice on approval of warrants under the Foreign Intelligence Surveillance Act, and we have had some concerns with the FBI standard, which we go into back in June of 2002 with Director Mueller. That is a very vital weapon in the arsenal. The Committee would like to know how long it takes and to be assured that you are really on top of that issue.

Director Mueller, on the so-called sneak-and-peek warrants, we have been provided with information just yesterday on some of the statistical data on the number of times these warrants were used. Sneak-and-peek means, for those who do not know, that there is no immediate notification given to the subject who has been the recipient of the search, of the secret search.

There are some 92 instances where the catch-all category of "seriously jeopardizing an investigation" was relied upon. There are in the statute a number of specific justifications for the delay, endangering life or physical safety, flight from prosecution, destruction or tampering with evidence, intimidation of a potential witness. The broad catch-all of "seriously jeopardizing an investigation" is so

broad that there are justifiable concerns that it can include practically anything.

Could that category be eliminated or could you look to the situations where you have used that catch-all to be specific and have specific items, such as the first four, which give definable parameters to this delayed notification?

Director MUELLER. Mr. Chairman, I do not believe that we would be well served by eliminating that provision. There are a number of circumstances that do not fit easily into the first four. An example is a recent case we had. It was a drug-smuggling operation from Canada in which individuals were bringing in a substantial amount of ecstasy from Canada. We had information, the DEA had information that this ecstasy was coming from Canada. They, quite clearly, did not want it on the streets, but they did not know all of the information as to whom it was to be distributed.

When these distributors came to the United States, they stopped at a restaurant. As they stopped at the restaurant and ate their meals, the agents, pursuant to a warrant, were able to enter the car, pull out the ecstasy so it would never reach the street, strewn glass around, indicating that the car had been broken into, and the individuals came back on their way. That ability to delay notification of that entry into the car allowed us to arrest 103, I think—somewhere over 100 persons who were involved in that conspiracy.

Chairman SPECTER. Director—

Director MUELLER. Now, the delay there was for less than 30 days, and it was pursuant to a court order.

The only other point I would make, Mr. Chairman, is that I think to characterize it as sneak-and-peek is wrong. It is a delayed notification. It is delayed notification that is pursuant to an order of the court.

Chairman SPECTER. Director Mueller, let me interrupt you to ask you to give specific illustrations. I like to be fact-specific, and the one you gave is impressive, and we would like more of them. We were provided information that one period was 180 days, and we want to get into the specifics of that, but I have only one second left, and I will conclude and yield now to Senator Leahy. I want to stay right on time.

Senator LEAHY. Thank you, Mr. Chairman.

I mentioned in my opening statement that the 9/11 Commission's report stated, with regard to extending the PATRIOT Act provisions, "The burden of proof for retaining a particular governmental power should be on the Executive."

Mr. Attorney General, do you agree that whenever possible the Government should make its case in public not in a classified report?

Attorney General GONZALES. Certainly, I believe that to be the case, Senator Leahy, that we have a responsibility to inform not just the Congress, but the American people, about the actions of its Government.

Senator LEAHY. I agree with you there. I noted that when Attorney General Ashcroft resigned, in his speech, he said, "The objective of securing the safety of Americans from crime and terror has been achieved." If we take that too literally, we do not need you, we do not need Director Mueller, we do not need the police officers

standing around this place. I know that you feel there is much work that still has to be done. I hope you will take a different tact than your predecessor and you will cooperate with this Committee as we consider how to improve upon and adjust the balances, we drew in the aftermath of 9/11 by way of the PATRIOT Act.

I believe that many of us would be willing to consider renewing some of the provisions that are subject to sunset, but you have got to have a sense of trust through greater accountability from the Department first.

I would like to see more and more regular reporting. Part of the difficulty with conducting oversight is the length of time it takes to get any information. Reports required by statute to be filed are months late or we never get them at all. For example, the PATRIOT Act required a report on the FBI's translator program, but that report was not submitted until late December 2004. Last Fall, we directed the FBI to issue a broader set of data by a date certain, September 14th, 2005 [sic]. It was submitted on the 1st of April, April Fool's Day, over 2 months late.

The Department has also been slow in responding to questions. Late last Friday, we finally received answers to questions submitted to Director Mueller a year ago, last May. We, also, received answers to questions that we submitted to Deputy Attorney General Comey after a PATRIOT Act hearing.

These are the reports and the outstanding hearing written questions and answers that were submitted between Friday, the 1st of April, and yesterday. I mention that because I do not think we would even have all of these. I mean, they come in at the last second, and they came in because we are having this hearing. If the Chairman had not scheduled it, I doubt if we would have had this. Some of them are over a year old.

And then sometimes it is hard to figure out how we do it. Look at these charts over here representing responses to FOIA requests over the past 6 months. The FBI has released the same e-mail in three different versions. The first version was released in response to the FOIA lawsuit on October 15th, 2004. It is almost entirely redacted. So, then, you come a month later, a second version, in response to the FOIA suit, it has fewer redactions, but still difficult to decipher. A third version was released the following year, after Senator Levin requested it, in redacted form.

Now, are the decisions of redacting made by the FBI or the Department of Justice? Because, obviously, three different decisions were made here on the exact, same document.

Attorney General GONZALES. Can I, first, respond to your earlier point about being responsive to congressional requests for information?

Senator LEAHY. I am complimenting you on getting these things in. They are a year late, but they are here.

Attorney General GONZALES. The good news is you did have an answer. The bad news is that it did take us too long to respond. I have had discussions with members of my staff to advise them that we need to do better. I understand that you need information to properly exercise your oversight role, and I am committing to you that we are going to do better. We have a new process in place so that we can respond in a more timely fashion.

But in defense of the Department, I am also aware that there have been extraordinary demands made by this Committee for information, obviously, within your right, but we want to be as careful and we want to be as forthright as possible, and it has taken us a great deal of time.

Senator LEAHY. But how, over such a short period of time, could you have such varying differences on this? I mean, who is making these decisions? Is it the Department of Justice or is it the FBI?

Attorney General GONZALES. I do not know specifically about these e-mails. I would be happy to look at them specifically and give you an answer, but, generally, of course, decisions made about how to respond to FOIA litigation, there are exemptions within FOIA which would allow the withholding of certain information.

Senator LEAHY. I helped write a lot of that FOIA legislation. I understand it. The reason I picked this particular one is because it is talking about the coercive techniques of the Defense Department's interrogations. It is interesting what was held out until a member of Congress really brought pressure. It said, "Results obtained from these interrogations were suspect at best." "Suspect at best" was the part being kept out. Why was that initially kept out?

Attorney General GONZALES. Senator Leahy, I really would like to study the e-mail and talk to the people involved in making that decision before answering that question.

Senator LEAHY. Will you answer the question?

Attorney General GONZALES. Once I have the information and feel that I can respond, give you some kind of answer, I am happy to do that.

Senator LEAHY. Article 3 of the Convention Against Torture states that "no state party shall expel, return or extradite a person to another state where there are substantial grounds for believing they would be in danger of being subjected to torture." Now, we are part of that treaty. What do you think the assurances we get from countries that are known to be torturers? When they say, well, we will not torture this person you are sending back, do you really think those assurances are credible?

Attorney General GONZALES. I think, Senator, that is a difficult question that requires sort of a case-by-case analysis. We have an obligation not to render people to other countries when we believe it is more likely than not they will be tortured. The President said we do not engage in torture, we do not condone torture, and we are not going to render people to countries where we think it is more likely than not they are going to be tortured.

Senator LEAHY. My time is up. I will come back to that because we do render them to countries that are known to be torturers.

Chairman SPECTER. Thank you very much, Senator Leahy.

Senator Kyl has had to leave to go to a leadership meeting, and he will be submitting a number of questions for the record. I turn now to our distinguished former Chairman, Senator Hatch.

**STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH**

Senator HATCH. Well, we welcome both of you to the Committee. Of course, the reason we wrote the PATRIOT Act to begin with was to provide law enforcement the tools that it needs that it did not

have in international terrorist situations. Many of these tools we already had with regard to the Mafia and other types of criminal activity, and so it was to update and bring the powers of our law enforcement people up-to-speed so that you could really go after international terrorists and domestic terrorists as well.

By the way, as I understand it, there is a 72-hour emergency time in which you can apply for a FISA warrant and get it, if it is an emergency, just so everybody understands that.

Now, much has been said, and much more will be said, about the effect of the PATRIOT Act on civil liberties. This is an important debate, but it is a debate that has to be guided by the facts, and the fact is that the critics of the PATRIOT Act are hard-pressed to provide documentation of any systemic abuse of the PATRIOT Act by the Department of Justice, the FBI or any other governmental agency. In fact, they are hard-pressed to provide any documented abuses of the PATRIOT Act. We have, I think, some 24 hearings on this issue and not one time have they been able to document an abuse.

Whenever a relatively new and complex law like the PATRIOT Act is implemented by tens of thousands of law enforcement officials, there is always a chance for some mistakes, even serious mistakes, to be made. I think we need to be vigilant so that we minimize the overzealous or improper uses of the PATRIOT Act. If we can improve this legislation, we ought to do so. I have been particularly heartened by you, General Gonzales, and by you as well, Director Mueller, that you are willing to look at some changes in the legislation that would tighten it up and make it better.

Now, in both of your prepared testimonies, you will note that Section 223 of the PATRIOT Act allows individuals aggrieved by any willful violation of the criminal wiretap statute or certain provisions of the FISA statute to file an action in Federal District Court to recover not less than \$10,000 in damages. Moreover, Section 223 also requires the Department to commence a proceeding to determine whether a disciplinary action is warranted against any Federal employee found to have violated the wiretap statute.

Now, the testimony of the Attorney General states, "To date, there have been no administrative disciplinary proceedings or civil actions initiated under Section 223 of the U.S. PATRIOT Act."

First, I want to make sure that I am correct in understanding that no actions have been brought, let alone have been successfully brought, under Section 223, in the three-and-a-half years since the PATRIOT Act has been on the books. Am I correct in arriving at that conclusion from your comments in your statement?

Attorney General GONZALES. Your understanding is correct, Senator.

Senator HATCH. That is fine.

Second, what do you think this record shows about how seriously the Department and the Bureau take their responsibilities to protect civil liberties as they engage in activities to identify and prevent terrorist acts?

Attorney General GONZALES. Senator, I think that that record indicates that we have tried to be careful in the exercise of these authorities. I think it, also, reflects the fact that I think Congress did a good job in drafting the PATRIOT Act and in including appro-

priate safeguards. We take those safeguards very, very carefully. We think they are very, very important, a critical part of the PATRIOT Act, and so I think that that is also reflected in this record.

Senator HATCH. Finally, going beyond the absence of cases filed under Section 223, can you tell the Committee whether you are aware of any documented cases of abuse of any provision of the PATRIOT Act?

Attorney General GONZALES. I am not aware of any documented case of abuse. I am aware that an organization yesterday released—we received a copy of a letter to Senator Feinstein relating to alleged abuses under the PATRIOT Act. It is a very lengthy letter. Obviously, we want to look at it very carefully in response to it, but based upon our cursory review last night, it appears that all of the allegations in that letter do not sustain the fact that there has been an abuse of the PATRIOT Act or do not even relate to the PATRIOT Act. But, again, I want an opportunity to study the letter carefully and prepare an appropriate response.

Senator HATCH. That has been my experience that most of the criticisms are of law enforcement not of provisions in the PATRIOT Act. They really do not apply. A lot of hysteria that has come from allegedly the PATRIOT Act violations really do not amount to anything and really cannot be justified.

I know that Senator Specter will be holding a hearing in a few weeks during which several critics of the PATRIOT Act will have the opportunity to testify about their concerns. So we will look forward to that and see what happens.

It would be helpful to the Committee if you would look into and provide us with a response to any specific charges of PATRIOT Act abuses that might be made at that hearing. So I would like to you to pay attention to that hearing and tell us as soon as you can about those particular abuses. Can we count on you to do that in a prompt manner?

Attorney General GONZALES. You can count on that.

Senator HATCH. Director Mueller, I think I have just enough time to ask this question. Your written testimony closes by making a plea for administrative subpoena authority in terrorist investigations. You note that Bureau has this authority in drug, health care fraud and child exploitation cases, among others, just to mention cases that are not terrorist involved. You, also, note that such a subpoena would be subject to challenge before the courts much like grand jury subpoenas may be challenged. Your testimony states, "In investigations where there is a need to obtain information expeditiously, Section 215, which does not contain an emergency provision, may not be the most effective process to undertake."

Now, let me ask you and the Attorney General two questions about this statement.

First, are you aware of any instances when a judge was not available to Act in a timely manner on a terrorism-related investigation? In other words, in short, is anything broken?

And, second, if it is, in fact, broken or might potentially be a problem in the future, why would an administrative subpoena provision be a preferable fix to writing an emergency judicial review provision into the statute, and why would it be better to have a neutral magistrate be involved before the subpoena or warrant was

issued if a suitable emergency review provision were crafted if such a provision is needed at all?

Director MUELLER. Let me respond, if I could, Senator.

Often we get information relating to threats, and we need to immediately find out whether that information is accurate or inaccurate, and we need basic records from third parties—hotel records. We may get information from the CIA or another agency that a person has come into the United States and is staying at a particular hotel in Washington, D.C., with an intent to link up with somebody else to conduct a terrorist attack in New York City. We need information from the hotel. We may even get the name of the hotel, and we need to get that information quickly.

Now, we have been fortunate much of the time to have the cooperation of the persons who run these hotels, motels or other such agencies where we need third-party information. But an administrative subpoena, which we utilize in narcotics cases, which Congress has given to us to utilize in narcotics cases, health care fraud cases, child pornography cases, a ream of other circumstances where we have the same need for third-party information, the administrative subpoena allows us to get that information very quickly so we can maintain the momentum of that investigation. An example is ISPs, relating to the use of the Internet.

The benefit of an administrative subpoena is that we can get it out, we can get it out there fast—the benefit to the Government. The benefit to the person who has been served with this subpoena is that they have an opportunity to challenge it before a court. They can talk to an attorney. They can challenge it before a court if they think it is unwarranted, not relevant to—unwarranted, let me just put it that way, or burdensome. So there is an advantage to us in terms of speed; there is an advantage to the recipient of the subpoena in terms of the ability to challenge it in court, as you would challenge a grand jury subpoena.

Chairman SPECTER. Thank you very much, Senator Hatch.

Senator Kennedy?

Senator KENNEDY. Thank you, Mr. Chairman, and welcome, General, and thank you very much, Mr. Mueller, for being here.

I would like to, Mr. Mueller, focus your attention on the detainee abuse in Guantanamo. On May 10th, 2004, the FBI e-mail described the Bureau's efforts to raise the concerns regarding the interrogation practices at Guantanamo Bay. According to the e-mail, the Defense Department interrogation techniques were so coercive the FBI was worried about using the statements produced by the interrogations in military prosecutions. The concerns of the FBI agents were echoed by U.S. Navy interrogators who were so outraged by the abusive techniques that had been approved by DOD officials that Navy officials considered withdrawing its interrogators from Gitmo.

Worse, the FBI e-mail describes DOD's refusal to stop using the coercive techniques even after it acknowledged that the information obtained through coercion was no more substantial than what the FBI got using simple investigative techniques, and the FBI pointed out that the coercive practices produced unreliable information. Further, the problem of using the coerced confessions to prosecute

the detainees was raised with the DOD General Counsel William Haynes, but it did not seem to make much of an impression there.

Do you know, from your own inquiry, whether anyone higher up in the Bureau passed its complaints on directly to either the Attorney General or the White House counsel or to the Secretary of Defense or initiate any criminal investigations of these kinds of activities? Did you have the opportunity to interview the four Justice Department lawyers named in the e-mail to see what they did with the information that you gave them?

Director MUELLER. My understanding is that persons in the hierarchy in the FBI did have conversations and, indeed, ultimately, we sent a letter to DOD reflecting concerns about certain instances that we had found, our agencies had seen at Guantanamo. There had been discussions, I would say, lower down in the Bureau with individuals at the Department of Justice with regard to appropriate techniques, particularly with regard to the understanding that FBI interrogations would be, according to our standards, would be necessary if we wished to prosecute an individual in the United States.

Now, in terms of an investigation, I did not undertake an investigation as to these four individuals who are listed in that e-mail. My understanding is that there were some discussions with regard to the techniques that were being used in Guantanamo with those persons at DOJ, and my understanding is those persons at DOJ had further discussions with the Department of Defense. We did, at one point, inquire of our agents what procedures they had witnessed that they believed to be beyond our purview, and we did provide that information to DOD for appropriate resolution.

Senator KENNEDY. So, as I understand, you had a communication with DOD. Is that the general counsel or do you know? Do you remember?

Director MUELLER. I think it was at lower levels both here at the Pentagon, but also down in Guantanamo. I know, in looking at some of the e-mails that have been passed, I know that there were discussions down at Guantanamo between our persons and the general who was in charge of either the base or at least the interrogation techniques.

Senator KENNEDY. Is that General Miller?

Director MUELLER. Yes.

Senator KENNEDY. I think the question is how are we going to ensure that the FBI is not going to be in the position of having to walk out of a room for fear they will be a witness to torture and who makes sure the prisoners are not tried and convicted on the basis of coerced statements that may be completely unreliable? How are you going to make sure that the FBI is not put in that position? How are you going to protect the Agency?

Director MUELLER. Well, from the outset, we have directed our agents to follow our standards. Our standards, from our book, is it is the policy of the FBI that no attempt be made to obtain a statement by force, threats or promises. From the outset, we have directed our agents to follow that standard. So we have followed that standard with the understanding that we may well be called as agents to testify in a court of law in the United States where the issue will be voluntariness and in the course of attempting to obtain a conviction.



Now, that does not mean that there are not other techniques that may be used by other entities that may well be legal, whether it be the CIA or the DOD. What I was concerned is that because our agents testify in the United States voluntariness is the standard, I attempted to assure that our agents followed that standard.

Senator KENNEDY. Just in that e-mail, it does point out DOD finally admitted that the information was the same information the Bureau had obtained. Is that basically your understanding?

Director MUELLER. I am not certain of the factual basis for that. I will say that it is tremendously important to get intelligence as well as providing a basis and predicate for going to court in the United States. We have had to modify some of our procedures, for instance, with regard to Miranda, when the circumstances are such that we would have to forego or use a modified Miranda and perhaps forego successfully having a person's statement admitted into a U.S. court in those circumstances where it is very important to gain intelligence as to future threats.

Senator KENNEDY. Let me move just to another area. This is on the GAO office found that a total of 44 firearm purchase attempts were made by individuals designated as known or suspected terrorists by the Federal Government from February 3rd to June 30th, 2004. In 35 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 immigration status within the federally prescribed 3 days.

In response to a recent inquiry by Senator Lautenberg and myself, other Senators, you indicated the Justice Department is convening a working group to study the GAO report and existing law and regulations. Should the FBI be in the business of authorizing the transfer of guns to people on terrorist watch lists?

Director MUELLER. Well, as we indicated in the response, the Attorney General has established a working group to look at that very issue. Persons may well be on a terrorist watch list without any disqualifying factor, and that is a factor that would disqualify them from getting a weapon, such as a conviction, such as an outstanding warrant, such as a stay away order. If that is the case, in these instances where GAO mentions that, and we become aware, as we would when we are alerted that somebody on the watch list wishes to purchase a gun, we then will pursue that. We will not let it go.

But in terms of whether or not there should be some modification to the regulations or the statute, the Attorney General has established a work group to look into that.

Senator KENNEDY. My time is up, but either the watch list needs addressing to be altered or changed, I would think. That is what we have for those individuals. We would have to ask is there a role really for the FBI for approving these matters.

I thank the Chair, and I thank the—

Chairman SPECTER. Thank you, Senator Kennedy.

In order of arrival, Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman. Thank you, General Gonzales and Director Mueller, for being here today.

Let me pick up, Director Mueller, with some of the questions that Senator Kennedy was asking you to make sure I understand

why it was the FBI did not believe it could use some of the DOD-approved interrogation techniques at Guantanamo.

I have traveled, like many other members of the Committee have, to Guantanamo and had a chance to talk to General Miller and see some of the detainees there and understand a little bit better about what was going on. As I understand, we were trying to do two things perhaps at the same time. One is to get good, actionable intelligence in a legal and appropriate manner that could help save American lives, either in the field, battlefield in Iraq, Afghanistan or here in America. That was one of the goals, correct, sir?

Director MUELLER. Absolutely.

Senator CORNYN. Also, there would be, under appropriate circumstances, an attempt to enforce our criminal laws, investigate violations of our criminal laws, past violations, and bring those to a court of law and seek to obtain a conviction of appropriate individuals; is that correct?

Director MUELLER. True.

Senator CORNYN. Just so I understand, the 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?

Director MUELLER. That is one of the reasons, yes.

Senator CORNYN. You talked about rules of voluntariness.

Director MUELLER. Yes.

Senator CORNYN. In other words, it has got to be a voluntary statement by the suspect; is that right?

Director MUELLER. Correct.

Senator CORNYN. For example, General Miller demonstrated to me when I was at Guantanamo how they would literally take a detainee from one location, I think, as I recall, three different places where they could be housed, but they would, on the basis of their cooperation, provide them better or perhaps food that they liked better. They could live in a group setting, as opposed to an individual cell, and that would be based on promises of cooperation and the like, certainly, not torture. But as I understood your testimony, it may impede a criminal prosecution because it may not be construed by a court in a criminal case as being strictly voluntary; is that right?

Director MUELLER. Perhaps.

Senator CORNYN. So the fact that the FBI did not participate in some of the interrogations conducted by Department of Defense or other officials, was that because you thought that they were engaging in a policy of torture or because you were concerned about your ability to obtain a criminal conviction based upon different standards in a court of law?

Director MUELLER. My understanding was that there were discussions elsewhere about the appropriateness of certain standards to be used by other agencies besides ourselves. I did not participate in those discussions. I understood that it was important to gain intelligence, but from the perspective of the role of our agents, it was to assist in interrogations, but to do so pursuant to the standards that we have employed in the past. There was some debate on the effectiveness of particular mechanisms. I think it is fair to say that

our agents were far more familiar in this area than I am. I believe that using the carrot rather than the stick often was more effective, but that was a debate that was ongoing.

Senator CORNYN. As I understood, you said it was against FBI policy to use promises as part of an inducement for people to give intelligence information or give information during an interrogation.

Director MUELLER. That is true.

Senator CORNYN. Yet that was one of the techniques used with great success at Guantanamo Bay to get information—

Director MUELLER. Good point, yes.

Senator CORNYN.—that has provided intelligence information and potentially saved American lives; is that right?

Director MUELLER. That is right.

Senator CORNYN. There have been some questions, of course, about the PATRIOT Act since it was passed three-and-a-half years ago. Of course, as I think Senator Leahy pointed out, of course, there has always been a debate about appropriate freedom and liberty interests and what we need to do in order to protect our security.

But let me ask you, General Gonzales, do you believe that the passage of the PATRIOT Act and its implementation by the Department of Justice, and by the FBI, and by other Government agencies is one of the reasons, one of the reasons, why al Qaeda and other terrorist organizations have been unsuccessful to date in attacking Americans on our own soil since September 11th?

Attorney General GONZALES. I do believe, Senator, it is one of the primary reasons because of the sharing of information, which both the WMD Commission and the 9/11 Commission have recognized is so very, very important. So I think it is one of the reasons.

I, too, like Senator Leahy and others here on this Committee, was involved in the drafting of the PATRIOT Act. We acted with deliberate speed because, quite frankly, we were concerned about a second attack, but we acted with a great deal of care and deliberation because we all understood that, while we needed to protect this country, we needed to do so in a way that was consistent with our values and consistent with the Constitution, and I think the PATRIOT Act reflects that balance.

Senator CORNYN. I agree with you that the PATRIOT Act is good work done under difficult circumstances, and I say that, in part, number one, it has been successful in at least contributing to the lack of a follow-up terrorist attack on our own soil as a result of some of its provisions.

But, secondly, it is true, is it not, General Gonzales, that the PATRIOT Act has been challenged numerous times in courts of law, and with the exception of the material support provision, which actually predates that controversy, predates the PATRIOT Act, there has been no provision of the PATRIOT Act held unconstitutional in a court of law; am I correct?

Attorney General GONZALES. There have been numerous challenges to various provisions of the PATRIOT Act, and I think, to date, that we have been successful in resisting those challenges. Some decisions have been made by courts and some people have—there is confusion as to whether or not was the provision chal-

lenged or struck down by the court really a provision of the PATRIOT Act. I think, if you study some of those decisions very carefully, you soon realize that they relate to provisions that were enacted by Congress years before the PATRIOT Act.

Senator CORNYN. I see my time is up.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Cornyn.

Again, in order of arrival, Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman.

First of all, with regard to the point Senator Cornyn was just making and the Attorney General was making, I want to clarify one thing about the recent decision striking down a national security letter authority that is expanded by the PATRIOT Act. The law that the court struck down was very different from the law passed in 1986. While the court focused on the lack of procedures, it was in the context of a law that allowed FBI agents to obtain records and even entire databases under a much different standard than was originally passed.

Mr. Chairman, I would say the Senator from Texas is simply not correct to say that the court struck down only the 1986 law. It struck down a law dramatically expanded by the PATRIOT Act. There is your example on the record of a provision of the USA PATRIOT Act that has been struck down.

Mr. Chairman, thank you very much for holding this hearing. I am pleased that we are beginning our review of the PATRIOT Act early in the year, and I want to thank you very much for your commitment to taking the time necessary to review the executive branch's exercise of Government power since September 11th. I am heartened that this year Congress will have the time and the perspective that we did not have in 2001 to carefully and calmly consider the many expanded Government powers in the PATRIOT Act.

As we all know, the PATRIOT Act was proposed days after the horrific September 11th attacks, and the bill was passed and signed into law just a little more than a month later. I tried, in that emotionally charged time, to convince my colleagues that some provisions went too far and needed to be revised, but my amendments were rejected, although, Mr. Chairman, I want to note that you supported me in some of those efforts, and I will always appreciate that.

Now, today, after three-and-a-half years of the Justice Department adamantly opposing any changes, and in some cases belittling critics, we have here today the Attorney General of the United States coming before us to this Committee to announce that he, too—he, too—recognizes the concerns about the PATRIOT Act are not so farfetched and that changes must be made. So we have come a long way.

Attorney General Gonzales, I wish this day had come sooner, but I am delighted. I need to understand more about the changes to Section 215 that you are proposing, since they were not mentioned in your written testimony submitted yesterday, and it is possible that we will disagree about whether your changes are adequate to address the concerns of the American people, but this is a departure from what we have heard before. It is a good start. Having

now taken this step, I hope we can have a productive dialogue that has been missing for so long.

I look forward to working with you, Mr. Chairman, and with our witnesses and with other members of the Committee as we embark on the reauthorization process, and I would ask that my full statement be printed in the record so I can turn to some questions. Mr. Chairman, I would just ask that my statement be put in the record.

Chairman SPECTER. Without objection.

[The prepared statement of Senator Feingold appears as a submission for the record.]

Senator FEINGOLD. Mr. Attorney General, I would like to ask you a bit more about a provision that you mentioned, the delayed notification or sneak-and-peek search warrants which were authorized in Section 213 of the PATRIOT Act. That provision, as you know, does not sunset, but has sparked a lot of controversy.

Before I start, I want to express a little frustration that the Committee received a lengthy letter just yesterday afternoon responding to some very longstanding requests for information about the use of the sneak-and-peek provisions. Given that we have only had a few hours to review that letter, I hope that you will agree to respond to any follow-up questions promptly.

Attorney General GONZALES. Of course.

Senator FEINGOLD. I want to clarify a few things regarding sneak-and-peek warrants that I think have gotten a little confused in the debate.

Mr. Attorney General, if the FBI were investigating an international terrorist or spy, it could obtain a secret FISA search warrant and never provide any notice to that person; that is correct, is it not?

Attorney General GONZALES. Generally, yes, sir—no notice under FISA.

Senator FEINGOLD. Section 213 has nothing to do with that authority one way or the other; that is right, is it not?

Attorney General GONZALES. That is correct.

Senator FEINGOLD. So, when we are discussing Section 213, Mr. Chairman, we are talking, for the most part, about searches done to investigate crimes that have nothing to do with terrorism or espionage, right?

Attorney General GONZALES. It can, but it also includes other kinds of crimes. That is correct, 213.

Senator FEINGOLD. There is no inherent connection to terrorism—

Attorney General GONZALES. That is correct.

Senator FEINGOLD. —vis-a-vis the power in Section 213 of sneak-and-peek.

Attorney General GONZALES. That is what Congress intended, I believe, when they drafted 213.

Senator FEINGOLD. I am glad we clarified that because I think many people have a different calculation about what they think should be permissible if we are talking about terrorism investigations. People should be clear Section 213 sneak-and-peek is, in no way, delimited to terrorist situations.

In the letter we received yesterday, the Department said that sneak-and-peek warrants are constitutional, in general, because of

a Supreme Court case *Dalia v. United States*. Let me remind you what that case says. It says that if the Government is planning to install a bug in someone's home, it can get a search warrant and delay notification because that is the "only means"—only means—"by which the warrant effectively may be executed."

Now, that is a pretty strict standard, is it not? Much stricter than the standard in the PATRIOT Act, right?

Attorney General GONZALES. I would like to go back and look at that decision carefully before I give you that answer, Senator, but I would be happy to do that.

Senator FEINGOLD. General, I can assure you there are various items listed as justifications under 213, and they are certainly broader than the language "the only means by which the warrant effectively may be executed."

I would argue that this is a much stricter standard than in the SAFE Act. Is that the standard that you think should apply to sneak-and-peek searches? And, if not, would you agree that the reliance on the *Dalia* decision is misplaced?

Attorney General GONZALES. Well, the standard that applies with respect to all of these kinds of warrants would be probable cause. That is the standard that applies here.

Senator FEINGOLD. As I understand it, this is a question of what circumstances allow an exception to the normal notice, and certain items are listed as exceptions. We may have a disagreement about what those exceptions should be, but all of this is certainly broader than the language of the *Dalia* decision, which speaks only in terms of only means by which the warrant effectively may be executed.

Attorney General GONZALES. Again, Senator, I have not read that case in some time, so I would like to opportunity to review it.

What people need to understand, though, with respect to 213, it requires a determination by a judge, first, that there is probable cause; secondly, that there is a reasonable cause to believe that providing immediate notice would result in some kind of adverse result. So this is not a decision made solely by the Government. This is a decision made by a Federal judge, finding a reasonable cause and an adverse result is going to occur.

Senator FEINGOLD. What we are talking about here, of course, are various provisions that are exceptions to what many of us regard as a constitutional protection. So the law in its current form and the proposals that we are making to change it all identify only certain circumstances where this exception can be made.

My suggestion to you, and I am happy to move on to the next subject so that you can review it, is that the *Dalia* decision does not even support that standard, let alone the type of standard that we are proposing under the SAFE Act.

Attorney General GONZALES. I would be happy to look at that, Senator.

Senator FEINGOLD. Mr. Chairman, my time has expired.

Chairman SPECTER. Thank you, Senator Feingold.

Senator SESSIONS?

Senator SESSIONS. Thank you, Mr. Chairman.

With regard to the 1986 Act and the debate about whether the PATRIOT Act was struck down, and I believe it has been discussed

here, Senator Cornyn, former Justice Cornyn, has written an op-ed that was published in the Washington Times and notes this, that what was struck down indeed was the 1986 Act, and in fact the ACLU, after contending otherwise, backed down and admitted that it attacked the wrong law. As ACLU attorney Jameel Jaffer eventually conceded, "The provisions we challenged and that the Court objected to were in the statute before the PATRIOT Act was passed. We should have raised the same objections before the power was expanded."

And in fact, Attorney General Gonzales, you never objected to the review and in fact thought it was implicit in the statute anyway, did you not?

Attorney General GONZALES. That is correct.

Senator SESSIONS. Let me just say this. I still contend that a myth has been created in large degree as a result of the talking heads on television that said we were going to have to erode our constitutional liberties to protect ourselves from terrorism. The Department of Justice, working with this Committee, crafted the PATRIOT Act and it was interpreted somehow as an erosion of our constitutional liberties when in fact it was never such, in my view. I predicted then that there was no provision of it that I believed would be struck down, and to date I do not believe any has.

The PATRIOT Act basically is a restrained piece of legislation that focuses on a number of loopholes and gaps in our law. Many times situations arise, as Mr. Mueller has noted, where the DEA can go out and issue administrative subpoenas in a drug case, the Food and Drug Administration can go into businesses and search everything in the business and get all kinds of documents, but an investigator investigating somebody trying to kill millions of Americans cannot do it. So what we did was try to give the same proven constitutional powers that existed in other investigations to people investigating terrorism and to break down the walls that had been created between intelligence agencies that made it far more difficult to share that information.

Am I wrong, Mr. Mueller, fundamentally in that—

Director MUELLER. No, I think you are accurate, sir.

Senator SESSIONS. And with regard to the delayed notification of a search warrant. Before you can get a search warrant, you have to get approval of a court and have probable cause that would justify you conducting that search. Is that not correct?

Director MUELLER. Yes, sir. In every case. Pursuant to the Constitution.

Senator SESSIONS. And if an FBI agent or a State police officer, if it is brought to your attention that they have conducted a search without a warrant, would you take immediate action against them?

Director MUELLER. The statutes require it.

Senator SESSIONS. And there is no doubt in the culture of law enforcement in America today—I say this as a prosecutor for 15 years—that you do not conduct searches without a court-approved warrant. Is that not correct?

Director MUELLER. That is correct except in a very limited area where there may be an emergency. But in every case that I am aware of, you have to go before a judge within a certain period of time to get approval of that action. It can only be an emergency.

Senator SESSIONS. And the FBI knows that and they do not do it. That is the point I am simply making.

Director MUELLER. Correct.

Senator SESSIONS. In 12 years as United States attorney, there was one wiretap that we were involved in. It is not a common thing to do a wiretap. You have to have a tremendous amount of proof and court approval and supervision.

But on this delayed notification, the so-called sneak-and-peek, basically all it says is that historically you issue a report or an inventory of the search and you give that to the person once you conduct a search warrant contemporaneously with the completion of the search. Is that not the traditional rule?

Director MUELLER. Correct.

Senator SESSIONS. But the courts have upheld in the past and it is an established principle of law enforcement since I was connected with the Department of Justice that you could conduct a search under certain circumstances with court approval and delay notification to the person who is being searched. Has that not been true?

Director MUELLER. Yes.

Senator SESSIONS. Before the PATRIOT Act.

Director MUELLER. Around the country, various courts have upheld that process over the years.

Senator SESSIONS. So this Act simply said we can do it when we are investigating people that are trying to kill us, not just sell drugs on the streets.

Director MUELLER. That, and it also regularizes the practice throughout the United States.

Senator SESSIONS. I think that is important for us to know here.

Now, they complain, and General Gonzales notes that perhaps the most controversial part is the part about the libraries. That is almost amusing. I mean, some of the things that have come out of the national Library Association, in my view, have been utterly extreme. It sounds like Woodstock myths, out of Woodstock or something. Library records, like medical records, like business records, have always been subject to subpoena. Is that not right, Mr. Mueller? You have been a Federal prosecutor for how many years before you became FBI?

Director MUELLER. Off and on for maybe 25 years.

Senator SESSIONS. And I would just say you are recognized as one of the most professional and able prosecutors in the Department of Justice, maybe in the history of the Department of Justice.

Director MUELLER. I would not go that far.

Senator SESSIONS. Well, I might. I might. Because I served with you and I know the reputation you had throughout the Department. So this is always—you can subpoena these records.

Director MUELLER. Yes, you can.

Senator SESSIONS. You tell me a principled reason why you could subpoena someone's medical records, their bank records, their telephone records, but not subpoena their library records. Is there one?

Director MUELLER. I do not believe so, and I do not believe there should be a safe harbor for libraries. We have had occasions where we have had terrorists who are operating, generally, computers. Many libraries now, public libraries, have computers that you can



have access to. And this has not been lost upon those who are affiliated with terrorist groups. We have had investigations in which we have seen persons associated with terrorist groups go into a library, use the library to communicate, or the computers in the library to communicate, draw up jihadist literature, and the like. We have been fortunate not to have used 215 because we have had the cooperation of the libraries to date. But the libraries can upon occasion be used for persons to communicate.

As I indicated, terrorists, we have had more than one—several examples where terrorists have used libraries as you would use a Kinko's or some other place to have access into a computer. We have also had occasions where, for instance, in the Kaczynski case, where the Unabomber, who was living in a remote area of the country but writing these tomes that would justify his actions in sending letter bombs, he utilized excerpts or quotes from various books. We came to find out that there was a library he was using, and we subpoenaed those records. It is in cases like that, cases where we have a belief, a predication that persons are using libraries in ways that will assist them in their illegal activities, where we believe that we should have the opportunity to address a subpoena of some sort to the library and have them produce records.

Senator SESSIONS. Thank you. And I know that they are entitled to every kind of constitutional protection, a library is, that anyone else is. But I do not think a library deserves a special protection over any other business.

Thank you, Mr. Chairman.

Director MUELLER. Could I add one other thing, if I might, Senator? We are sensitive to the concerns of the Library Association. But all that being said, we think that the balance is well struck in terms of our need to obtain records from a library. If it is 215, a judge is reviewing that request. And so the balance is fairly struck, I believe, in terms of the desire of librarians and others to protect the sanctity of the library.

Senator SESSIONS. A library does not have any sanctity. Why does a library have sanctity that your medical records do not have?

Director MUELLER. Well, a number of areas have been looked upon as being special.

Senator SESSIONS. They think it is sanctified, I will admit. I just disagree that it deserves special protection.

Chairman SPECTER. May we move on, gentlemen?

Senator Schumer?

Senator SCHUMER. Thank you, Mr. Chairman. And I want to thank both the Attorney General and the Director for being here today.

I am going to start off with—Senator Kennedy mentioned it briefly—the issue of terrorists and guns. I think both of you would agree with me that in order to fight an effective war against terror, common sense dictates we must not only take care to arm ourselves with the proper legal tools, but we ought to disarm terrorists as well. And you are familiar that all of us learned, unfortunately, last month from the GAO report that we are not doing everything we can to disarm terrorists. Forty-seven times, it was reported, people on terrorist watch lists legally purchased guns in the U.S.

Even worse, it would be bad enough if this were accidental, but it is not. Even if the FBI wanted to prevent a suspect terrorist from buying a gun, even if the watch lists were perfect—because I know you alluded to the fact that maybe the watch lists are not perfect—the FBI could not, could not prevent a terrorist from buying a gun. If you are on a terrorist watch list today, that fact is not enough under current law to be denied a deadly firearm. So what that means, it leads to an absurd conclusion. If somebody is convicted for some nonviolent crime, like illegally selling lottery tickets, he cannot even buy a revolver. But if he has sworn allegiance to al Qaeda, he can stock up on AK-47s and Uzis to his heart's content.

What troubles many of us, of course, is the substance, but is also—it is completely out of touch and out of tune and out of consistency with what this administration does on every other issue. So when it comes to the age-old clash between security and liberty, the administration instinctively sides with security, except in one area—guns. Guns are inexplicably a sacred cow. And you have to wonder why this is. Is it politics? Is it the power of the NRA? As you know, I agree with the President that we should have a strong offense on the war on terror. But we should be going after the terrorists in every way when they prepare to strike us and not make a huge exception for guns. By the same logic that the administration has pressed over and over again, if we prevent garden variety criminals from possessing firearms, why do we not prevent suspected terrorists from possessing them? I do not understand that.

So that is why Senator Lautenberg and I wrote a letter to the Department demanding action, asking that gun-purchase records, rather than being destroyed within 24 hours, are kept for a longer period. I also have to tell you, I am going to plan to introduce an amendment to this bill that would, once and for all, make it illegal for people on terrorist watch lists from getting guns. In addition, because I support Senator Lautenberg's efforts to keep gun records, I plan to offer in Committee an amendment to prevent the destruction of gun sales so that we do not hamper our ability to trace terrorists.

First, to Secretary Gonzales, would you consider, would the administration consider supporting legislation to prevent those on watch lists from buying guns?

Attorney General GONZALES. Well, let me be very clear about this, Senator. The administration does not believe and would prefer not to have, desperately prefer not to have terrorists possessing guns. And we do what we can to make sure that that does not happen. But at the end of the day, we have to enforce the law. And unless someone has a disability under the law from possessing a firearm, then they are entitled under the law to possess a firearm. And so we have taken steps, also reflected in the GAO report, to try to buy some additional time—

Senator SCHUMER. Mr. Attorney General, I am asking you, would you support, would the administration just consider supporting changing the law?

Attorney General GONZALES. We would certainly consider looking at your legislation, of course.

Senator SCHUMER. You would not rule it out?

Attorney General GONZALES. That is correct.

Senator SCHUMER. Good. Thank you.

Second, that would relate to terrorists not getting guns when they go into the gun shop. But sometimes you find out that someone is a terrorist after they have purchased the gun. I think we have had that in a few instances as well. That would mean that we would have to keep the records for at least a longer period of time. Your predecessor instituted a policy where the records were destroyed in 24 hours. Would you consider supporting legislation that would require the records be kept for a period longer than 24 hours, particularly—Well, let me ask you that.

Attorney General GONZALES. We would be happy to look at your legislation. My own sense, it is not the fact that the records are being destroyed in 24 hours that is sort of the main problem, it is the fact that it is currently not a disability from owning a firearm. But we would be happy to consider your legislation.

Senator SCHUMER. Well, but this is an example. I mean, Joe Smith goes into a gun shop, buys a whole bunch of guns legally, and then it is found out later that he was on a terrorist watch list. If you destroy the records—well, you will not be able to find out later, if you destroy the records. That is why we want to keep the records. No one wants to use them for any other purposes. So I would urge you to consider that as well. That is a possibility?

Attorney General GONZALES. We would consider that.

Senator SCHUMER. Good. Because your predecessor had instituted the previous policy.

And just in reference to what Mr. Mueller said—and I share the respect for the FBI Director that my colleague from Alabama does—you were alluding, when Senator Kennedy asked you questions, well, we are not sure the watch list is perfect. I thought that is what you were saying, the watch lists have some problems. Well, we use them for lots of other things—not getting on an airplane, things like that. You are not saying we need a standard of perfection in the watch lists before we use them to prevent people who are on them from buying guns, are you?

Director MUELLER. No. What I meant to say is there are people on the watch list who do not suffer from any of the disabilities that would preclude them from having a weapon. In other words, there would be information that leads us to believe that a person is affiliated or associated with terrorism. We put him on the watch list, but that person will not necessarily have that—

Senator SCHUMER. You mean will not have a criminal record.

Director MUELLER. Will not have a criminal record, will not have—

Senator SCHUMER. Right. But we do not require a criminal record for airplane boarding or anything else. Why should we allow people like that to buy a gun? Any good reason?

Director MUELLER. No, all I was saying, that the watch list should not be the—Well, the watch list serves certain functions. It does not serve the function of assuring that everybody on there has the debilitating factor—

Senator SCHUMER. Well, that is not what it is supposed to be, as you know. It is a totally different list.

Director MUELLER. That is true.

Senator SCHUMER. There are people who are not American citizens on that list.

Director MUELLER. That's the only point I was trying to make. Chairman SPECTER. Senator Schumer, your time is up.

Senator SCHUMER. Thank you, Mr. Chairman.

Chairman SPECTER. Director Mueller, I want to return to a subject I raised in my opening statement, and that is the report of the Commission on Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. No matter how effective the PATRIOT Act will be, we know that, unless there is information sharing among the intelligence agencies, we have a gigantic gap in our security system. And we do know, and have talked about this extensively, about the tremendous amount of information which was available before September 11th, about that Phoenix FBI report which never got to headquarters, with the fellow who wanted to learn how to fly a plane but was not interested in take-offs or landings. And we had Agent Coleen Rowley's report about the wrong standard being used on Foreign Intelligence Surveillance Act that never got to the headquarters of the FBI, and she was in this room back in June of 2002 and we had extensive discussions about that. And we know the CIA had information about al Qaeda agents in Kuala Lumpur, never given to Immigration and Naturalization Service. And we know about Zacarias Moussaoui, part of the Agent Rowley issue as to the information which might have led to total disclosure of the al Qaeda plans.

And then we had the legislation to create the secretary of homeland security, and Senator Lieberman and I, co-authors, fought hard to get a provision that would give direction to the secretary and we could not get it done. The House passed the bill in October of 2002 and, as they do from time to time, left town, so that we were faced either with taking their bill or deferring the matter until the spring. Now we have the creation of the national Counterintelligence Center, and of all the specifics on the war against terrorism, it is my view, having chaired the Intelligence Committee and done a lot of oversight on this Committee, that that coordination is the most important and without it, we are desperately vulnerable. One of the first things I did after taking over the chairmanship was to come to see you to clearly get into that subject. Because I think we can be helpful on oversight.

Let me say this to you, Attorney General Gonzales, there is a lot of experience on this panel. There are prosecuting attorneys, there are lawyers with a lot of experience, or jurists, who have been in the field a long time. So that it was with really some dismay that I saw the report of the Commission on Intelligence Capabilities Regarding Weapons of Mass Destruction again referring to clashes between the CIA and FBI not only in regard to what agency gets credit for an intelligence report, but also in the field, where lives are at stake. And then the failure of the CIA and FBI to cooperate and share information adequately on cases could potentially create a gap in the coverage of these threats like 9/11. And there are a lot of references. And, only to cite one more, in-fighting between the FBI and the CIA had "become too common" and that "potential information on terrorism sometimes was not shared among the FBI, CIA, and Department of Homeland Security."

Director Mueller, are those criticisms outdated?

Director MUELLER. I think, if you focus on what the WMD Commission was looking at, some of it was accurate, particularly when it comes to the sharing of information between our Legats overseas and the CIA station and the sharing of information and the working cooperatively between the NR stations and the FBI here. We are well on our way to resolving those coordination issues.

On the other issue of sharing information with regard to—

Chairman SPECTER. Director Mueller, when you say “well on your way,” it has been a long time since 9/11 and it has been a long time since June 6th, when you and I were here together, and a long time since October, when Senator Lieberman and I tried to get it under one command. Now, we do have a new national Director of Intelligence, but he has not been confirmed and it will take him awhile to get operational. And who can say that, assuming confirmation of Director Negroponte, that he is going to be able to solve the problems?

Director MUELLER. If I might, Mr. Chairman, in the sharing of information between the CIA and the FBI when it comes to terrorism, we have made huge, huge strides. I am not certain that the quotes that you are stating would accurately reflect our exchange of information on terrorism. We have established a national Counterterrorism Center—

Chairman SPECTER. So the quotes are wrong?

Director MUELLER. I would say they do not accurately describe the full picture of what we have done since September 11th to assure cooperation between the FBI and the CIA. And I mentioned the national Counterterrorism Center, where we gather information in the United States pursuant to our procedures—the CIA gathers it overseas—and we have used it in the national Counterterrorism Center. We have colocated certain of our international terrorism units with similar units with the CIA, and the exchange of information there is as good as it possibly could be.

Chairman SPECTER. Director Mueller, let me ask you one final question before my 36 seconds expire in this round. There are reports about critical information which led the administration to conclude that Saddam Hussein had weapons of mass destruction and it came from somebody named Curveball, or nick-named Curveball. And then the reports are that the information from Curveball never got to CIA Director Tenet. And then there are reports that the information from Curveball never got to Deputy Director McLaughlin.

Now, during my stewardship here, I am going to put everybody under oath when we have testimony, as we do on confirmation hearings. But I am just aghast at the necessity for Congress to pursue these issues as if we are after John Dillinger, as to who knew what and when.

Director MUELLER. Well, I am disappointed as well, Mr. Chairman.

Chairman SPECTER. That is not your watch.

Director MUELLER. I am disappointed as well, Mr. Chairman, that you feel you have to do that.

Chairman SPECTER. Senator Leahy?

Senator FEINSTEIN. Mr. Chairman, I think you—

Chairman SPECTER. Pardon me, Senator Feinstein. Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

General, I want to thank you for the report that you sent, which I have received and have been poring through. I think it is very helpful, and we have given a copy of it to each member of the Committee. As I understand it, you go through each section—I am talking mainly now about the 16 sections subject to sunset—with respect to the use, and it varies rather dramatically. Sections 201 and 202, you say, have been used maybe once, maybe twice. And you get to 203(b) and 203(d), which involves the wall, and they are quite frequently used. And I wanted to ask you about it.

As you mentioned in your comment a little earlier, the ACLU has written a 10-page letter, which is rather specific, particularly on page 8 and 9, on some specific what they contend are abuses of the PATRIOT Act. Now, we have scrubbed the area once again and we find—I have no reported abuses. I had 21,000 reported abuses when we started this. We have asked the Inspector General for abuses, and he has not come up with any.

So I think the situation is very different today as opposed to what it was when we passed the act. I think, for one thing, PATRIOT II, which was reportedly going to come to the Hill following PATRIOT I, did not. And I think that has become clear. I think people's understanding of the Act is much clearer today. I think there are still misimpressions around 203(b) and (d). And the ACLU letter, because I authored in this Committee the significant purpose test, I want to ask you a question specifically about that test and the Brandon Mayfield case, using it as an example.

Can you describe how the significant purpose test was used in this case? I think it is a good example because it is both a criminal and an intelligence matter.

Attorney General GONZALES. Senator, I think we have said publicly—if not, I guess I am saying it publicly—that the PATRIOT Act was not used in connection with the Brandon Mayfield case. The search was not conducted pursuant to Section 213. The question that you are raising is whether or not 218 is implicated in terms of, quite frankly, which change the purpose test from “the” purpose to “a significant” purpose. The truth of the matter is, the facts as I understand the Madrid bombing and the investigation with respect to Mr. Mayfield would have been an investigation that we could have pursued, quite frankly, irrespective of the change to the PATRIOT Act. It would have been—we think that it was a—you could make the argument that the purpose of that investigation was for purposes of foreign intelligence. And so for those reasons, we disagree with the conclusion by the ACLU that the provisions of the PATRIOT Act were implicated in connection with that investigation.

But again, I have only had a short period of time to review the letter. I do not have the letter with me. My staff is looking at it carefully. Obviously, when anyone alleges any kind of abuse, we consider it very, very seriously. We know you consider it equally as serious, and we want to be as responsive as quickly as possible to reassure you that in fact the Department's actions have been consistent with the law.

Senator FEINSTEIN. I guess what I would like to know, since this is an oversight hearing on that, whether the significant purpose test, you believe, at this stage is adequate—is it an adequate protection; if we should change it in any way

Attorney General GONZALES. I truly believe it is important. I think it is adequate in that I think it has been successful in aiding the Department in its investigations, and so I do believe it is adequate. I do believe it is important, and I do believe that, again, as I said earlier in response to a question, in my judgment, the PATRIOT Act includes a lot of safeguards that critics of the Act choose to ignore. They don't talk about the safeguards that do exist in the Act.

I think they, as I said before, reflect a very careful balance between the security of this country and the protection of our civil liberties, and for that reason we wholeheartedly support the renewal of the PATRIOT Act.

Senator FEINSTEIN. If I might ask you if you would take a look on pages 8 and 9 of the ACLU letter, they raise some specific cases—Michael Galardi, the case of a lovesick girl who planted threatening notes aboard a Hawaii-bound cruise ship, the case of Czech-born University of Connecticut grad student Thomas Faral, David Banash—and make the general allegation that sneak and peek, 213, was used almost exclusively outside of terrorism investigations.

You might not be able to address those with specificity today.

Attorney General GONZALES. I can say, Senator—

Senator FEINSTEIN. If you can, that would be great.

Attorney General GONZALES. Well, as to the specific cases you referred to, I would like the opportunity to go back and look at these carefully, but Section 213, the delayed notice warrant provision, was not limited only to terrorism cases. So the fact that that authority was used in connection with other kinds of cases doesn't mean that we violated the law.

Quite to the contrary, the Department acted pursuant to the law. We exercised authority that was granted by this Congress, but I welcome the opportunity to study these allegations further and we will report to you as quickly as we can.

Senator FEINSTEIN. I appreciate that. Thank you.

Mr. Mueller, let me ask you this question. I am concerned—and I have asked this question of you before—that there is insufficient understanding of the difference between intelligence and law enforcement.

How many senior DOJ officials who are running national security today are professional intelligence officers?

Director MUELLER. We have not had a certification program in the past. So in terms of a certified intelligence officer, we do not have anybody. We are in the process of establishing a certification program.

I would have to get back to you in terms of numbers of persons at the top levels who have spent a substantial amount of time in either counterintelligence or throughout their careers have spent time in the intelligence community, whether it be a year or two at the CIA or had some form of training that would qualify them to be a certified intelligence officer.

Senator FEINSTEIN. Just quickly because my time is up, could I ask the same question of you, General, please?

Attorney General GONZALES. I don't know the answer to that, Senator, but I would be happy to get that information for you.

Senator FEINSTEIN. Mr. Chairman, I think this is a real problem. I suspect the answer is zero. Going back to the Rob Silberman report and putting on my Intelligence Committee hat, I think there is a growing view that there needs to be a specific national security division under an assistant attorney general for national security which is really intelligence-driven.

The question comes really whether you can change the culture sufficiently, and I asked this question at a prior hearing and the answer has always been zero. And the question comes whether we can really get in this country that corollary to MI-5 with the structure that is set up today. I thought originally that we can. I must say I am beginning to doubt it now. The fact that this new commission once again came up with that same recommendation is something we need to look at.

Thanks very much.

Chairman SPECTER. Senator Feinstein, I think you have put your finger on a very critical issue. The commission recommended a national security division for both the FBI and the Department of Justice, and that is a subject which I plan to take up in the next round and I think it is a very important subject to be discussed.

Senator FEINSTEIN. Thank you.

Chairman SPECTER. Senator Coburn was just here, but we will go to Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman.

Gentlemen, we are talking, of course, about the PATRIOT Act, but I want to pull back a little bit more and look generally at our efforts to protect America from terrorist attacks and specifically talk about the border. This causes me a great deal of concern, and let me explain.

While I think we have done a great job since 9/11 upgrading our means of determining who can come into the country and why they are here through the implementation of the US VISIT program, upgrading the quality of documents, identifying people who are presenting fraudulent documentation and the like, I fear that we are not doing what we need to be doing between the bridges and outside of the airports. Let me just explain.

A few weeks ago, I flew with a Border Patrol agent in Laredo, Texas, down the Rio Grande River and landed on the World Trade Center Bridge, and asked about whether he was receiving the kind of support they needed in order to do their job. He said no, that because of demands along the Arizona border, the Texas border was seeing a move of equipment and personnel to Arizona.

He said, what I fear is that the human smugglers are smart enough—and it is not just human smugglers, it is human traffickers, it is drug dealers, money launderers, arms dealers and the like—to move to a different part of the border and our borders are way too porous.

So I would just like to get your opinion, General Gonzales, on whether this is a concern of yours from a terrorism point of view,



from a national security point of view, the porous nature of our borders.

Let me just mention one little footnote. On my most recent trip to Laredo, I was also provided with some documentation in the way of pictures of juice boxes with Arabic writing on the juice boxes that did not come from that area where the person was detained and where the juice boxes were obtained, and also a jacket with Arabic writing on it, some of a jihadist nature, including a patch showing a plane flying into a large building. These were just a couple of the sorts of things that are being obtained in the course of detaining people coming across our border from Mexico.

So I would just appreciate your general observations, Attorney General Gonzales, about whether you are concerned about that from the standpoint of protecting America from terrorist attacks.

Attorney General GONZALES. Well, of course, I am concerned about opportunities that terrorists have to come into this country. There is a tension between the principles that we hold dear about being an open society, encouraging immigrants into this country, and also the principle of defending this country against terrorists that come to this country simply to do evil.

Like our President, I come from your State, Senator, that borders Mexico. We understand the realities of life along the border communities where people come back and forth everyday not to do harm, but simply to provide for their families. So an immigration policy, in my judgment, has to be reflective of that reality as well.

So you have got these competing tensions of the reality of life along the border, the need to protect this country, and also I think the principle which many of us believe in and that is that if we have immigration laws, they should be enforced. That should be, of course, a principle that we all support.

So to answer your question, am I concerned about it, of course I am concerned about it, even though the responsibility regarding immigration enforcement now lies within the Department of Homeland Security. I know that Secretary Chertoff shares the same concern and he is working as hard as he can, along with the rest of us, to try and address this problem.

Senator CORNYN. Let me ask you, would it make your job and Director Mueller's job easier if, in passing comprehensive immigration reform, we were able to distinguish between people who wanted to come to the United States and work on a temporary basis and then return to their home country—distinguish between those people and those who want to come here to kill us?

It just strikes me as a logical matter that, given the limited resources of law enforcement, no matter how vast people may think the Department of Justice is and how vast the Federal Government's resources are, would it help if you were able to concentrate on people who were likely threats to American security, as opposed to people who wanted to come here to work under some legal framework?

Attorney General GONZALES. Of course, it would help that we know who is coming across our borders and the reason that they are coming into this country. The President has proposed a worker program that contemplates providing some kind of legal status to

certain people who meet certain qualifications, and I think that is consistent with the approach that you are thinking about.

Senator CORNYN. Director Mueller, let me just ask—consistent with, I think, the questions that Senator Leahy was asking, I am very interested in the Freedom of Information Act. He and I have cosponsored a couple of bills that we are hopeful of getting action on in the Committee and then on the floor.

Specifically, I am concerned about why would you see three different versions of the same e-mail with different decisions made about redaction. It concerns me that it may be just happenstance who requests what at what time, and we lack any coordinated effort to determine exactly what statutory exemptions do apply and to make sure that those are uniformly applied to each and every request for the same information.

Director MUELLER. I would have to go back and look at how the various iterations were developed. I do know there are different standards for FOIA. There may be different standards for classification. I don't know to what extent in this sequencing either one or the other kicked in to address one or more of the provisions. I would have to get back to you on that.

Senator CORNYN. Well, I would appreciate when you are responding to Senator Leahy's questions about that if you would also include a response to that. I would like that both from General Gonzales and Director Mueller because I think getting some systematic, uniform response in a predictable way that provides people the information they are entitled to, while protecting information that is entitled to a legal exemption, is important.

Thank you.

Chairman SPECTER. Thank you, Senator Cornyn.

Senator Leahy commented that someone had two rounds before one. We have had a practice of alternating between the parties. I know we go to Senator Durbin next, but maybe we ought to rethink the issue as to whether we avoid the alternation in the interest of giving people a first round. I will give due consideration to that.

Had we done it earlier, you would have been up sooner, but it is your turn now, Senator Durbin.

**STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR  
FROM THE STATE OF ILLINOIS**

Senator DURBIN. Thank you, Mr. Chairman.

Thank you, Attorney General Gonzales and Director Mueller, for being with us today. I think we should start this conversation about the PATRIOT Act, this dialogue, by acknowledging the obvious. Let's be honest. We passed the PATRIOT Act at a moment when our Nation was gripped with high emotion and fear.

History tells us that we don't do our best work under those circumstances. I think we know that we don't enact laws with adequate and careful consideration under those circumstances. Sadly, history tells us we often err on the side of expanding the power of government at the expense of individual rights and liberties.

That is why if there was any wisdom in this PATRIOT Act, which I voted for, it was the sunset provision which said we will revisit these things; we will determine whether or not we are caught up in the emotion of the moment and have gone too far.

I think it was in that spirit that Senator Craig and I took a look at the PATRIOT Act and suggested the SAFE Act, which does not repeal or abolish the PATRIOT Act, but adds what we consider to be thoughtful provisions which are going to make it more specific in what it sets out to do, and more protective of the rights of individuals.

Now, if you search the political spectrum in the Senate, you will probably find no two Senators farther apart than Senator Craig and myself, and you will find the groups supporting our SAFE Act as diverse as well, from the American Conservative Union to the American Civil Liberties Union.

So I am heartened by your opening statement, Attorney General, about being open to suggestions and ideas. It is a grand departure from your predecessor and I think it is the right spirit for us to address the PATRIOT Act. And I would commend to you, as I am sure Senator Craig would, the provisions which we are offering.

There are two things which I would like to speak to specifically about the PATRIOT Act and what has been said this morning. The very first reason, Attorney General, that you gave for the PATRIOT Act was to enhance the Federal Government's ability to share intelligence. That is an absolute necessity for our defense of America in the war on terror.

But most honest observers will tell you that to suggest that the only way we can expand the sharing of information and intelligence is to expand the power of government, or to at least move perhaps too far when it comes to individual rights and liberties, overstates the obvious.

We now know, well documented by investigation after investigation, that there was a bureaucratic turf war in many agencies which stopped them from sharing information. Director Mueller has devoted more hours than he can count to improve the outmoded technology he inherited after 9/11 so that information systems could communicate.

The point I would like to make is this: If the goal here was, as you say, to enhance the Federal Government sharing intelligence, we could have stayed away from the PATRIOT Act altogether and really focused on the agencies working with one another and sharing information so that the Phoenix memo wouldn't be buried in the depths of the FBI and so that the CIA and all the other agencies would communicate.

So before we go to challenge in any respect the Bill of Rights, I think we had a lot of homework to do when it came to the management of information in the Federal Government. Maybe this new intelligence reform will move us in a more positive direction.

The second thing I would like you to address is Section 215, which has caused great pain for people in many communities. The American Library Association, not historically a politically active group, has become very active because they believe the PATRIOT Act went too far.

They believe, for example, if an FBI field office believed that an unidentified terrorist had checked out a book entitled How To Build a Dirty Bomb from the Chicago public library, Section 215 gives the Government the authority to search the library records of hundreds of ordinary citizens in an attempt to identify the ter-

rorist, catching in this net innocent people who have checked out books in a library, never knowing that they would be swept in the potential of finding a terrorist.

Similarly, if an FBI field office came up with information that the wife of a suspected terrorist had an abortion, therefore they would set out through Section 215 to search the records of a hospital or clinic for all the women who had received an abortion, whether or not they might have been associated with any terrorist activities. Section 215 allows all of that information to be gathered in secret through the FISA court and many innocent people to have their privacy compromised in the process.

Now, often, it is said that we should stop and consider that it is just like a grand jury subpoena, but it is not. There are significant differences. The recipient of a grand jury subpoena can challenge the subpoena. That is not the case here. The Government must make a showing with a grand jury subpoena of the need before a gag order is imposed. That is not the case here.

The Section 215 provision of the PATRIOT Act is in secret, and the recipient of the subpoena can challenge the gag order, which can't be done under Section 215. So the analogy breaks down completely when you try to argue that this is just a routine process like a grand jury subpoena.

So I wish you would address Section 215 in that context. If, in fact, the records of a library should be protected and are somehow sacred, can the same not be said for medical records and other business records that might be swept up in the same Section 215 effort?

Attorney General GONZALES. Thank you, Senator. You bring up some, I think, good points. Obviously, Section 215, in my judgment, has been subject to a great deal of misunderstanding, and let me repeat what I said earlier. This Department and the Government has no interest in the library reading habits of ordinary Americans.

We do believe, however, that libraries should not become safe havens for people who are here in this country and do want to do harm to other Americans, and we do have evidence of that happening even though Section 215 has not been used in connection with library records. We do know that there have been examples of terrorists who are using access to computers at libraries.

As I said in my statement, we do believe that there is an inherent right, but would support a change in the law to allow specific challenges to a Section 215 order, and would support changes in law that would allow someone to talk to an attorney in connection with preparation of that order.

My own sense is that there are sufficient safeguards that many people choose to ignore, and that is let me just mention a few. This is not just the Government making this decision. We have to go to a Federal judge. That judge—

Senator DURBIN. But Section 215 requires the judge to issue the order. It is required. I can read it to you, but I know you are familiar with it. The language says specifically, "Upon application made pursuant to this section, the judge shall enter an ex parte order." There is no discretion.

Attorney General GONZALES. Once the U.S. Government presents information meeting the relevant provisions of the statute, you are

right; the law does provide that the judge shall issue the order. But I quarrel with those who have characterized this as a rubber-stamp operation. We provide information to the judge. Judges often ask questions. Judges often ask us to go back and get information. We provide that information and then the judge makes the decision.

Senator DURBIN. The information is not individualized. That is my concern and Senator Craig's concern. You are not talking about a person suspected of; you are talking about a potential group of people that includes many innocent people. It is as if you said we have the authority to arrest and search large groups of people in hopes of finding one criminal.

Under our system, there is more particularity required, is there not? And Section 215 does not include that.

Attorney General GONZALES. There is, in our judgment, a relevance standard that should be applied in connection with 215, relevance to terrorist activity or an intelligence investigation.

Senator DURBIN. But is it individualized? Is it individualized?

Attorney General GONZALES. It is certainly applied as narrowly as we can, and people have the opportunity, Senator, after the fact—if the information is going to be used in any way in any kind of proceeding, they have the opportunity to go to another judge and contest the collection of that information.

Finally, I might remind you that we do have an obligation upon the Department to provide semi-annual reports about the exercise of this authority. So it is not true that the Department is using this authority in secret.

Senator DURBIN. Do you provide that information to the Judiciary Committee?

Attorney General GONZALES. I don't know if it is—

Senator DURBIN. The answer is no. You give it to the Intelligence Committee. You don't provide the information to the Judiciary Committee, as I understand it. Is that correct, Mr. Chairman? I see my time is up.

Chairman SPECTER. Well, we are counting this on your second round, Senator Durbin.

Senator DURBIN. I am going to stop, then. Thank you very much.

Chairman SPECTER. You are well into your second round, but we kept you waiting a long time. So under equitable considerations, we are giving you that extra time.

Senator DURBIN. Thank you. Thanks for stopping me, too.

Chairman SPECTER. Besides that, you are on a subject of great concern to the Chairman.

Senator DURBIN. Well, many of my colleagues are waiting to ask and I won't dwell on it, but I wish we would receive more particular information than generic numbers. I think it might be more helpful.

Thank you very much.

Chairman SPECTER. Senator Leahy.

Senator LEAHY. Well, I agree with the Senator from Illinois. We might have reports, but, one, if we get them, usually we get them late, if we get them at all, and oftentimes they are meaningless. The fact is, no matter how much a judge might ask questions, the law says he shall give the order.

I thought we left some of my questions up in the air earlier. And that may have been the time constraints, so let's just go back to it. Going back to the 2001 State Department report on Iraq which was talking about Saddam Hussein, it says the security services routinely and systematically tortured detainees. According to former prisoners, torture techniques included branding, electronic shocks administered to the genitals and other areas, beating, pulling out fingernails, burning with hot irons and blow torches, suspension from rotating ceiling fans, breaking of limbs, and denial of food and water.

Now, under those circumstances, suppose we had had a detainee here and we had Saddam Hussein's assurances that he would not be tortured if he was rendered back to Iraq. Does anybody think we would have rendered him back? We would not have relied on his assurances, would we? I realize it is a hypothetical, but I can't imagine we would.

Attorney General GONZALES. Senator, I think you present sort of an extreme hypothetical. Obviously, we would look carefully at the record of the country in terms of how they have dealt with other individuals that they are holding in their custody. We would look at the record of the other country in how they have met their other commitments to this country.

Senator LEAHY. Before we get too far into the hypothetical, are you suggesting that there is anybody in any administration that would have rendered somebody back to Saddam Hussein under his assurances?

Attorney General GONZALES. I am not suggesting that, no, sir.

Senator LEAHY. Okay, so let me ask you about another area. We have, however, relied on assurances from Uzbekistan that they would not torture detainees transferred from U.S. custody. Now, I am going to read somewhat similar words to cover the 2004 State Department human rights report on Uzbekistan.

Quote, "Police, prison officials and the NSS allegedly used suffocation, electric shock, rape and other sexual abuse. However, beating was the most commonly reported method of torture. Authorities frequently and systematically applied torture, including severe beating, suffocation and electric shock."

Do you think that Uzbekistan's promise that they would not torture detainees is trustworthy or even credible?

Attorney General GONZALES. I think a country that would have that kind of record, we would have to receive some very special assurances to satisfy ourselves in meeting our legal obligations that it is more likely than not that someone that we sent over in their custody would not be tortured.

Senator LEAHY. Well, the President in his March 17 press conference was asked a question and he declined to answer. Perhaps you can answer it. What is it that Uzbekistan can do in interrogating an individual that the United States cannot?

Attorney General GONZALES. What is—

Senator LEAHY. What is it that Uzbekistan can do in interrogating an individual that we might send there that the United States cannot?

Attorney General GONZALES. I don't know how to answer that question, Senator. I do know that the policy of this country is that we will not engage in torture or condone torture.

Senator LEAHY. I know that. We are not going to condone torture. We have this unmarked—actually, “unmarked” is probably not the best way to describe the CIA planes because you can go on the Internet and you can find out which places they have landed and taken off. They won't tell us, but you can easily find it on the Internet.

We say we won't torture this person, but we put him on the plane and send him to a country that does torture. I am not sure that we really have standards. I mean, if our standards are to rely on their assurances that they won't torture somebody, do you really think, with some of the countries that we send detainees to, that that is an adequate assurance?

Attorney General GONZALES. Well, again, Senator, we take this obligation very, very seriously and we know what our legal obligations are. We know what the directive of the President is, and each case is very fact-specific.

Senator LEAHY. That is going to be great comfort to the Canadian citizen sent to Syria and then being tortured.

Attorney General GONZALES. Senator, with respect to that particular case, I think he was—he wasn't rendered. I believe he was deported.

Senator LEAHY. He was not allowed to continue to Canada once he got into the United States, even though he was a Canadian citizen.

Attorney General GONZALES. He was also a Syrian citizen, I believe, sir.

Senator LEAHY. I know. A lot of people have dual citizenship, but if he had had a dual citizenship with a lot of other countries, we would have sent him on to Canada.

Would you support legislation to make diplomatic assurances an insufficient basis for determining that a detainee would not be in danger of being tortured if he was rendered to another country?

Attorney General GONZALES. Senator, I would certainly consider legislation. I believe that the administration is currently meeting its legal obligations.

Senator LEAHY. In mid-January, you opened a wide-ranging investigation into reports from the FBI about the military's use of coercive and abusive tactics against prisoners held in American custody at Guantanamo Bay and in Iraq.

What is the scope of the investigation and when is it expected to be concluded?

Attorney General GONZALES. Senator, there are, as you know, a series of investigations about the potential abuses that have occurred in various theaters of operation. Some investigations are here in Congress, some within DOJ, some within DOD, some within CIA. All those are at various stages of progression.

I have asked folks within the Department to try to get a sense of where things stand. I have already received one report and I am waiting for additional information to get an assessment of how these investigations stand.

Senator LEAHY. Will you let us know when you hear?

Attorney General GONZALES. I will be happy to share with you what I think I can, sir.

Senator LEAHY. Director Mueller, has the FBI transferred detainees to other countries, and if so, which countries?

Director MUELLER. I don't believe so, in the context in which you are saying it, which I presume is—

Senator LEAHY. No, not in the context in which I am saying it. Have you transferred detainees to other countries?

Director MUELLER. I don't believe so.

Senator LEAHY. Will you double-check that?

Director MUELLER. Yes.

Senator LEAHY. I am not asking about a country that might torture or not. I am just asking if you have transferred detainees to other countries.

Have you been asked to?

Director MUELLER. I would have to get back to you on that. I don't believe so.

Senator LEAHY. If you are asked to, do you have a process of determining whether the person may be tortured if they are sent to another country?

Director MUELLER. We would do that in conjunction with the Department of Justice and with the Immigration Service if that is indeed the case.

Senator LEAHY. The Weapons of Mass Destruction Commission report says, we have been assured that it is currently the case that the Attorney General personally approves any interrogation techniques used by intelligence agencies that go beyond openly published U.S. Government interrogation practices.

Is that accurate?

Attorney General GONZALES. I can really speak with certainty about the actions of this Attorney General, Senator Leahy, and I can say that I am personally involved in providing—

Senator LEAHY. Can or cannot say?

Attorney General GONZALES. I can say that I am personally involved in providing legal analysis and legal approval with respect to techniques.

Senator LEAHY. Have you personally approved the use of any extraordinary interrogation techniques?

Attorney General GONZALES. There has been no decision to date with respect to that, sir. The answer to your question is, no, I have not.

Senator LEAHY. Thank you, Mr. Chairman. I will have other questions later.

Chairman SPECTER. Thank you, Senator Leahy.

It is now almost noon. As announced earlier, we would run until one and come back this afternoon. We have a little more than an hour until one o'clock, so we have time for eight rounds. Perhaps we will be able to finish by one o'clock. I know that would be a relief to the Attorney General and to the Director, who have a lot of other duties, and also to members. So we will see how we progress.

Senator Hatch.

Senator HATCH. Thank you, Mr. Chairman.

One of key challenges in fighting terrorism is to share information among various governmental agencies. This was one of the



central conclusions of the 9/11 Commission report. The recent WMD Commission report also made this point and singled out the FBI as an entity that could do better in sharing information.

I think that there is widespread agreement that one of the major benefits of the PATRIOT Act was, as both of you have noted in your testimony, the manner in which Sections 203 and 218 acted to take down the wall that had previously existed between intelligence and law enforcement personnel.

I would like both of you to tell the Committee about the efforts underway by each of you personally and your agencies to see that information is shared across the Federal Government, as well as with relevant State and local law enforcement officials and appropriate international partners in our worldwide battle against terrorism. In particular, I would like both of you to tell us how you share information with the CIA and other agencies within the intelligence community.

Let me also say that I recognize that Ambassador Negroponte is not yet been confirmed as Director of national Intelligence, but I would like to know how you personally and institutionally plan on working with him and his office, with CIA Director Goss and with Secretary Chertoff, as well, to make certain that President Bush and other decisionmakers have all the available information they need and that the Congress can be assured that the DOJ and FBI are sharing information in a timely and comprehensive manner.

So if you could both talk to that, then I have maybe one other question.

Director MUELLER. Let me just start with what we have established since September 11th. We started with a small intelligence office and have now built it into an intelligence directorate with several thousand intelligence analysts. One of the components of that is the development of reports officers. At last count, I had something like 183 reports officers whose responsibility it was to take information, strip off the sources and methods, and distribute that information and disseminate that information throughout the community, whether it be the intelligence community or State and local law enforcement, DHS.

So as opposed to the presumption prior to September 11 that you did not disclose something unless there is a good reason, the presumption now for us is you disclose unless there is a good reason not to disclose.

They will field intelligence groups in every one of our field offices. Those field intelligence groups include analysts and agents whose responsibility is to gather intelligence, but to do assessments as well as disseminate intelligence. So within the FBI we have developed a structure that we are still—I would agree with the Commission that we are still in the process of building it. We are not where we need to be, and we have a ways to go. But we are in the process of having an intelligence directorate that includes analysts, surveillance officers, language specialists, targeting officers, agents that will perform that intelligence function.

With regard to the DNI, we would expect from the DNI, from Mr. Negroponte, taskings with reporting back, taskings to fill gaps that are perceived in the intelligence that is necessary to be gathered within the United States.

With our fellow agencies, we have—as I indicated before, we have the national Counterterrorism Center, which combines access to all of our databases. There is access to the FBI databases, the CIA databases, DHS databases, DOD databases in this particular national Counterterrorism Center. We also have colocated elements of our counterterrorism division with comparable elements of the CIA and others so that they are sitting side-by-side, which will give us better coordination on transnational intelligence operations. That is a baseline that we have established for the exchange of information. We still have a ways to go, but I think we have made substantial strides.

Senator HATCH. I think you are doing a terrific job up to that part, so I asked the question. I wanted to make sure that this is—I know you have had some criticisms, some of them unjust, some that may be just, in the sense that you are still not there. But you are working at it very hard.

Let me just ask you both another question. I understand that the ACLU has run a television advertisement claiming that Section 213 of the USA PATRIOT Act allows law enforcement to search our homes “without notifying us,” implying that this provision gave Federal law enforcement the authority to conduct searches without ever providing notice to the individual whose property is searched. I would like to know if this is an accurate description of the so-called what you have criticized, I think adequately, search-and-peek, to use their language, provision. And am I correct in reading your report yesterday, this provision has only been used 155 times since 2001?

Attorney General GONZALES. The ads are incorrect. We are required by law to provide notice in each and every case.

Senator HATCH. So. So this is just typical of the efforts made against the USA PATRIOT Act. Am I correct?

Attorney General GONZALES. You are correct in that we are required to provide notice, Senator Hatch.

Senator HATCH. Okay. Well, Attorney General Gonzales, I take it from your testimony that you would not be averse to writing into Section 215 an explicit relevancy standard. As I understand it, you believe a probable cause standard to be too high a burden in the investigatory stage, and at our fielding hearing in Utah last year, Deputy Attorney General Comey suggested that the relevancy test was de facto employed by judges under Section 215. So I am pleased that you have signaled today that the Department is prepared to make what has been implicit explicit.

So I just want to compliment you on that and compliment both of you. You have tough jobs. It is easy to sit back and take cheap shots at you, as many have done. But you folks have done as good a job as anybody in my 29 years now in the United States Senate has done, and you, General, in the short time you've been in there, but you, Director, have been in there ever since right after 9/11. And I just want to compliment both of you. We all know that things are never going to be perfect, but by gosh, you have both tried your very best to get them as perfect as you can and I want to personally let the whole world know just how good you really are.

Director MUELLER. Thank you.

Attorney General GONZALES. Thank you.  
Chairman SPECTER. Thank you, Senator Hatch.  
Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman.

First, with regard to the point that Senator Hatch was making, it is certainly accurate that the statute under Section 213 does provide that there has to be notice within a reasonable period. But I do want it noted that that opens the possibility of a much longer period of time than what the various circuits have suggested. I understand that the three circuit courts have suggested 7 days. So the concern here is that it is a vague, potentially unlimited period for notice and I just want that noted in the record.

Attorney General GONZALES. May I make a comment to that, Senator? I am told that the average time in which case the delay occurs is between 30 and 90 days. The other thing that I think people need to remember is that this is a determination by a Federal judge as to what is a reasonable period of time, depending on the circumstances that that judge is confronting.

Senator FEINGOLD. Let me move on. Mr. Mueller, just a quick follow-up on Section 215. The Attorney General said, I am sure accurately, that Section 215 has not been used to obtain library records. But I believe you mentioned earlier that libraries have voluntarily cooperated with the FBI, making it unnecessary to use Section 215. Can you clarify that? It sounds like they have given up library records, but you did not need to compel them under Section 215.

Director MUELLER. That is true. I mean, we have had in circumstances where librarians understand the, I would say, discreet inquiry and we've had occasions where, several occasions where in the course of terrorism investigations we have had to obtain library records. I only make that point to say that because we have not been forced to go to 215 does not mean that we have never had occasions where we have needed to go and obtain library records.

Senator FEINGOLD. I think that is an important clarification. Now it is clear on the record that library records have been obtained pursuant to these investigations. There are people out there on both sides distorting this issue, and I am pleased to say that it can no longer be said that library records have never been obtained, although not under the force of Section 215. But they have been obtained pursuant to investigations—voluntarily requested and obtained pursuant to terrorist investigations.

Director MUELLER. Yes, and on other occasions there had been sufficient predication for a possible criminal charge so that it may have been under the force of a grand jury subpoena.

Senator FEINGOLD. General Gonzales, as you know, 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 by clarifying that the pen trap authority applies to the Internet as well as to phone communications. It makes sense to apply the same rules to all types of communications, especially as technologies converge.

The line between content and non-content information is simply harder to draw, as you know, in the context of Internet communica-

tions. In the telephone world, it is somewhat easier. The phone numbers dialed are not content but the actual conversation is; but in the Internet world there are gray areas. For example, it is unclear whether a URL, which indicates exactly where a person has gone on the Internet, is content that requires a full wiretap order. I understand from Deputy Attorney General Comey's recent 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.

How does the Justice Department evaluate whether an aspect of Internet communications such as a URL constitutes content under the statute?

Attorney General GONZALES. Senator, this is a very—for me, because of my limited computer knowledge—complicated area. And you are right, it does raise, in my judgment, complicated questions. And I think it is appropriate to ensure that content is not being collected whenever the authorities under 214 are used. I do not have a specific answer for you. I can get that information for you. But I wanted to reassure you that, first of all, to acknowledge what we all know, and that is that this is a very—can be a complicated question; and also to reassure you and the rest of the Committee that we care very much about ensuring and having in place mechanisms so that we are not collecting content. Because that is not—214 is not about collection of content.

Senator FEINGOLD. Thank you, General. I look forward to working with you on that issue.

Director Mueller, I understand that FISA evidence is far more frequently introduced in criminal prosecutions in the post-September 11th, post-PATRIOT Act era. Is that a correct statement?

Director MUELLER. I would have to check on that. It may well be. I do not have any way of knowing it without going back and actually looking at that and trying to determine what the incidence was beforehand and the incidence afterwards.

Senator FEINGOLD. Well, that is my understanding. We can talk about the specifics of it later. But I also understand that because of the strict standard currently in FISA, no criminal defendant has ever gotten access to the underlying surveillance application or order. That stands in sharp contrast to the introduction of criminal wiretap evidence at trial, where the wiretap law requires, of course, that defendants receive the full application and order so that they have the opportunity to challenge the underlying basis for that order. Is that a correct statement, that there is this difference between FISA and normal—?

Director MUELLER. Yes, that is a correct statement. But there is a judge that reviews it. In other words, a trial judge does review the adequacy of the presentation under the FISA laws for the issuance of the FISA order. So it is not as if it is not reviewed. It is reviewed by the trial judge.

Senator FEINGOLD. Fair enough, but if secretly collected FISA evidence is going to be increasingly used in criminal trials, I think we have to provide defendants with adequate opportunity to contest those orders. While your agents do a very good job, we also know that sometimes they make mistakes. People like Brandon Mayfield have been incorrectly targeted. And the FISA court, which

also does an excellent job, does not benefit from an adversary process. Would you agree that before FISA evidence is used to prosecute people and put them in jail, defendants should get access to the reasons the Government had for secretly wiretapping their phone conversations or searching their homes, taking into account the need to protect classified information?

Director MUELLER. No, I would not.

Senator FEINGOLD. You do not agree that they should get—

Director MUELLER. No. I would say that the judge who is in charge of the case should review the application. It is not just the evidence that may be presented, it is the capabilities we might have, all of which, in my mind, in the interests of national security, need to be protected. And I do believe that the trial judge who is evaluating the case against the defendant is in an appropriate position to balance the national security needs against the request of the defendant and his counsel to have access.

Senator FEINGOLD. Well, my time is up, but let me simply say, Director, I hope we can continue talking about this. I am not suggesting the judge should not play that role, but I am suggesting that the defendant should have a right to have the basic information he needs to let the judge know what his side of the case is so the judge can do the proper balancing.

Director MUELLER. Well, I think in the context of the criminal case, the defense counsel can and have—

Senator FEINGOLD. I am talking about the FISA.

Director MUELLER. About FISA. They understand that if FISA is out there, they are—they know the case against them. They are absolutely, and have in the past filed arguments as to why they should have access to the FISA. And the court has reviewed those and found them wanting.

Senator FEINGOLD. What I understand is they are not given adequate information to know that, but we will take that up another day. Look forward to working with you.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Feingold.

Senator SESSIONS?

Senator SESSIONS. Director Mueller, the principle that we worked on for many years in this country—it is fairly settled—is expectations of privacy. Courts have asked that question, fundamentally where there is not an expectation of privacy, subpoenas are adequate; where there is an expectation of privacy before the subpoena or administrative or grand jury is issued, the court must approve it, and that becomes a warrant requirement. Now, under FISA, I think you have made it pretty clear but I think it is important for us to talk about it one more time. Under FISA, the only thing that is unusual here is that the person on whom the subpoena is served does not have a right to object and go to court over that, because it is presumptively dealing with national security in a matter of sensitivity. Is that correct?

Director MUELLER. That is correct, sir.

Senator SESSIONS. But before that—but the review is conducted before the subpoena is issued. A judge must approve that kind of subpoena before the FISA must approve it, before it is issued. Is that right?

Director MUELLER. Correct.

Senator SESSIONS. But normally under grand jury subpoena or an administrative subpoena, a recipient of that can object and move to quash the subpoena and not produce the documents. Is that right?

Director MUELLER. That is correct.

Senator SESSIONS. So under these administrative subpoenas that the FBI has been giving under the Privacy Act, if someone thinks they should not produce the records, they can object and having a hearing on it, and not produce the items.

Director MUELLER. That is correct.

Senator SESSIONS. And not produce the items. Administrative subpoenas, again, are very common in the history of our country and existed all the time I was a prosecutor. Would you explain some, list some of the examples where administrative subpoenas are available today in non-terrorist cases, far less serious cases than these?

Director MUELLER. I think there are a number of various agencies that have—I think somebody mentioned the FDA already, but in narcotics cases, in health care fraud cases, in child pornography cases, sexual exploitation cases. You can rattle off a number of cases or areas in which administrative subpoenas have been accorded by the Congress understanding the necessity of getting that information and providing to the individual upon whom the subpoena is served the opportunity to contest it if they so desire.

The one point I would make is that these are subpoenas to third parties for records and the like. These are to third parties for records and the like.

Senator SESSIONS. That would require somebody to produce something out of their home, out of their locked glove compartment, inside a letter that has been addressed to them. All of those require a court-ordered warrant on probable cause, not relevance.

Director MUELLER. Correct.

Senator SESSIONS. Is that right?

Director MUELLER. That is correct.

Senator SESSIONS. You are looking, I think—

By the way, do you know of any law—of course, under this act, libraries are not mentioned in any way, shape, or form by name, are they?

Director MUELLER. No, not at all.

Senator SESSIONS. Do you have any citations for your authority that there's a sanctity of the library?

Director MUELLER. I meant to say that there is perceived-by—librarians sanctity. I do not believe that it is written in the law anywhere.

Senator SESSIONS. Well, they are not—I understand their desire to avoid unnecessary perusal of people's library records, but I am certain, as you said, that the FBI has no desire to scan everybody's library records. They have more to do than that.

Now, there is a question about, under certain circumstances, the ability to forbid disclosure. It used to be banks and hotels and motels would produce documents and the agent or the local police detective would ask them not to tell the person because they were conducting an investigation, and they would not. My understanding

from my experience in prosecuting is that more and more lawyers have told these banks and motels and other businesses that they can or should report any subpoena of the person's record. And this could have a very damaging impact on a very sensitive investigation, could it not?

Director MUELLER. Without a question of a doubt. The disclosure of interest in an individual who is being targeted prior to indictment would result in the destruction of evidence quite often, perhaps a fleeing from the jurisdiction, and avoiding justice as a result of a filing of an indictment and charges once the investigation is complete.

Senator SESSIONS. Now, Mr. Mueller, let us say you are investigating a terrorist cell in an area of this country and you have probable cause to believe that there is legitimate approval of probable cause to believe that at least one or more individuals have critical evidence inside a motel room. Can you explain to the average American why it might be necessary in the course of that investigation not to immediately disclose to the renter of that motel room that you have been in the room to examine whether or not evidence is there that might identify other people or the crime that is ongoing.

Director MUELLER. Let me give you an example that happened overseas, an investigation in which we were working with others. I learned that there was a substantial quantity of ammonium nitrate in a storage locker. Come to find out from an informant that there is a substantial amount of ammonium nitrate in the storage locker which is to be used for a substantial terrorist attack. At the time, at that point in the investigation the investigators did not know who were the co-conspirators, who had ordered it, who was going to carry it out, whether there was a vehicle available. But they did know that there was ammonium nitrate in a storage locker, a substantial amount that could be used for an explosion.

Assuming that had come in the—if that was in the United States where we came across this information of ammonium nitrate in a storage locker but still had to continue the investigation, we would go to court and get an order to go in and seize that ammonium nitrate, replace it with an inert substance, delay notification so we could continue the investigation to determine who had ordered that this plot be undertaken, who was paying the rent on the storage locker, and continue the investigation so that we could take out not just that ammonium nitrate in the storage locker but all of those who were involved in that terrorist plot. And so the delay of notice would be absolutely instrumental in that occasion to assure that we could wrap up those who intended to harm the United States.

Were we not to have that and we had to give notification to the owner of that storage locker, we would have to perhaps not even be able to arrest that person because we would have insufficient information to arrest that one person, much less all of those who were involved in the plot.

Senator SESSIONS. And all of his buddies would scatter like a covey of quail.

Director MUELLER. Absolutely. As soon as you go in with police and seize that—in plain view go in and seize that ammonium ni-

trate, not only would, quite obviously the press would pick up on it very quickly and everybody would be in the wind.

Senator SESSIONS. And that is done on drug cases.

Director MUELLER. In drug cases—

Senator SESSIONS. Before the PATRIOT Act was passed, you could do that in drug cases?

Director MUELLER. Yes, and I think I gave the example of Ecstasy coming in the country, where we didn't want the Ecstasy distributed. And yet the investigation was not completed, and so we went through a ruse. We seized the Ecstasy but continued the investigation, leading to the arrests of over a hundred individuals who were involved in the plot. That is the importance of the delay of notification.

Senator SESSIONS. I think it is critical. We cannot allow that to be eroded.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Sessions.

Senator Feinstein?

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Mr. Mueller, I wanted to clarify our prior round of questions here. In 2003, the Intelligence Authorization Bill contained language which mandated the DCI prepare standards and qualifications for intelligence officers. It is now 2005. When was this mission completed?

Director MUELLER. I am not certain. Within the Bureau, the mission was completed, I believe, December of 2004.

Senator FEINSTEIN. So you did receive the standards and qualifications?

Director MUELLER. Well, I would have to see to what extent our Intelligence Officers Certification Program is dependent on standards and qualifications from the intelligence community. I know we have completed our Intelligence Officers Certification Program as of December of last year, if that is what you are referring to. Maybe I am confused.

Senator FEINSTEIN. Well, it is my understanding that the DCI has not complied with the law. If you would—

Director MUELLER. We will check on that.

Senator FEINSTEIN.—please find that out and let me know—

Director MUELLER. I will.

Senator FEINSTEIN.—I would appreciate it very much.

Director MUELLER. I did not mean to, in my answer to your previous question, Senator, leave the impression that we have not built up a substantial cadre of intelligence specialists within the FBI. We have. And we have an intelligence directorate now of several thousand persons, including analysts, agents, surveillance, language specialists in the intelligence directorate. What I was referring to is the specific certification has not been done, but I did not want to leave the impression that we have not taken substantial strides in response to the legislation the President has directed to establish the intelligence directorate we have.

Senator FEINSTEIN. I appreciate that very much, and I know you have made those strides. I just want to see that the intelligence end has been complied with, and I do not believe, based on what I know, that it has.



I would like to ask a question on the roving and John Doe wiretap, if I might, Mr. Attorney General. Section 206 creates roving wiretaps which allow the Government to get a single order that follows a target from phone to phone. In addition, the Intelligence Authorization Bill, passed shortly after the PATRIOT Act, allows the Government to issue John Doe wiretaps, where the phone or facility is known but the target is not known. The way that the two laws were written seems to allow for a general wiretap, one that follows an unknown suspect from unknown phone to unknown phone.

Does this mean that you could get a John Doe wiretap to listen to all the telephones in a certain area? I realize that sounds physically impossible, but just for a moment assume the technology is there. Does the law as written give you that authority?

Attorney General GONZALES. The short answer is no, Senator. Before I follow up on that answer, I cautioned earlier about the ACLU and the fact that we had not had a great deal of opportunity to look at it. You asked me specifically about the Mayfield case, and I am advised that there were certain provisions of the PATRIOT Act that apparently were used, specifically the information provisions were used, the 207 authorities were used, which extended the duration of the electronic surveillance, and I am told in some sense 218 was used, although quite frankly I am not sure in what sense it was used, since I was told the contrary last night. So I did not want to leave you or the Committee with a misimpression about that. Obviously we will look into it further and give you the most accurate information.

Senator FEINSTEIN. I really appreciate that. I think it is important, since this has become an issue that we clarify exactly where it is.

Attorney General GONZALES. As to your question about roving wiretaps, we believe there is an obligation with respect to Security 206 to either identify the person by name or to provide some type of specific description about a particular individual, that the authority is to be used with respect to a specific target and that, if for some reason we were mistaken about the target—we now say, well, this is the guy we really want to go after—we have to go back to the court and get an additional authority under 206. I also believe that there is—

Senator FEINSTEIN. Beyond what point? Beyond what point would you have to get additional authority? How wide would the tap have to be?

Attorney General GONZALES. I was referring only with respect to any event that we had concluded that we had the wrong target. It is not a case that 206 could be used on one person and then we could simply use that authority to tap the phones of another person. It is target-specific, and 206 does give us the authority to either identify the target by specific identity or by some kind of specific description to the court.

Senator FEINSTEIN. So once you have identified the authority, you cannot use that tap in any other capacity in that area. Is that correct?

Attorney General GONZALES. We cannot use that tap with respect to another target.

Getting to the second prong of your question about the scope. Could we simply go up on phones in, you know, an entire city because, you know, a person might be in the city, there is a limitation that we have some reasonable basis to conclude that a set of phones is either being used or is going to be used by that specific target. So I think that there is that limitation on the law as well.

Senator FEINSTEIN. But it is a pretty broad authority. I could see it being construed to use it in a very wide area.

Attorney General GONZALES. It may be viewed as a broad authority by some, but I would like to remind you and the Committee again, it is a probable cause standard. Both prongs have to meet a probable cause standard and we have to satisfy a Federal judge. And so we present information to a Federal judge and satisfy the probable cause standard that in fact we have a specific target and we could limit the scope of the surveillance.

Senator FEINSTEIN. Thank you. I would like to ask you about the definition of domestic terrorism in the bill. Section 802 defines it. As I understand the definition, it is any actions occurring primarily within the United States if they involve a violation of State or Federal law; secondly, appear to be intended to influence Government policy or civilian population by intimidation or coercion; and three, involve acts dangerous to human life.

Now, some contend that this is a very broad definition and thus expands the type of investigative conduct law enforcement agencies may employ. Because of the chilling effect that this might have, there is concern. My first question would be how would you justify such a broad definition. And the second question is if you could explain how the words appear to be intended or are understood by your Department.

Attorney General GONZALES. I think that, first of all, let me begin by saying that, of course, this does not create a crime of domestic terrorism. It simply provides a definition of domestic terrorism to be applied with respect to a variety, a number of other statutes.

Concerns have been raised with respect to this particular provision that it may in fact chill organizations and groups that want to, you know, protest and march against this Government, things of that nature. That is why the law was written the way it was, so that we are talking about actions that were already in and of themselves violations of some other criminal statute and also about those kinds of actions that would involve the actual endangerment of human life. And therefore the kinds of protests that we see from time to time here in Washington would clearly not be covered within the definition of domestic terrorism.

Senator FEINSTEIN. Except by the vagary of the way the statute is worded. You use the term "involves loss of human life," but that is not necessarily correct because it is a broad statement, as I understand it, of "any violation of State or Federal law," not just State or Federal law that involves a threat to human life.

Attorney General GONZALES. My understanding, Senator, is that both of those—that all three would have to be met, is that there would be a violation of a statute, action intended to influence or protest Government actions—although that second prong, I would

have to look at the statute specifically—but the third prong as well, as to endanger human life.

Senator FEINSTEIN. Thank you for that explanation. Could you explain the words “appear to be intended” and how they are understood?

Attorney General GONZALES. I do not—I would like the opportunity to get back to you on that, Senator.

Senator FEINSTEIN. I can understand that.

Okay, thank you very much. If you would, I would appreciate it.

Attorney General GONZALES. Yes, ma’am.

Senator FEINSTEIN. Thank you. Thank you, Mr. Mueller. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Feinstein.

The national Security Division, which we talked about a little earlier, has been a recommendation of the national Commission which reported last week. I frankly have grave doubts that it is a matter of restructuring, but I would be interested in your views, Attorney General Gonzales, as to whether you think restructuring would really be relevant and germane or the issues are much more substantial. And similarly with you, Director Mueller.

Attorney General GONZALES. Mr. Chairman, even before the report came out, I directed that there be a review within the Department as to whether or not we should look at restructuring. As the WMD Commission report indicated, we are probably the only Department that has not engaged in any kind of restructuring following the attacks of 9/11—Main Justice, I am referring to. I think that there are, certainly one could argue there are good reasons why a restructuring would make sense. Let me preface my remarks by saying that there’s been no decision, and obviously we would want to consult with the Congress about a possible restructure and get their views.

But in the interagency process I feel that sometimes the Department is not as well represented as it should be often. If I am not available or if the Deputy Attorney General is not available, then it really falls down to sort of a deputy assistant attorney general, and sometimes that is probably not the best representation for the Department and some very important decisions have to be made on the interagency process.

We now have—in my judgment, the Criminal Division has a great deal of responsibility. More and more personal attention is required with respect to counterterrorism and counterintelligence issues, and one has to question whether or not it would make some sense to move certain operational responsibilities out of the criminal division. You have the counterterrorism reporting up to one deputy assistant attorney general, counterespionage into another deputy assistant attorney general, and I do not know if that is the right way to structure it.

So it is something that we are looking at very seriously.

Chairman SPECTER. Why has that not been done up till now?

Attorney General GONZALES. Sir, I do not know why it has not been done up to now. I suspect that people have been focused on exercising other authorities to protect this country.

Chairman SPECTER. Director Mueller, what do you think about it? Is it necessary? Would it really make a difference for you, your unit?

Director MUELLER. Well, the concerns the WMD Commission pointed out are very valid and they are substantial. In terms of our building up the capabilities to an intelligence structure. And when they point out that the Office of Intelligence is weak because it does not have budgetary authority, it does not have control over certain of the analysts, they are absolutely right. We have to build up an intelligence capacity within the Bureau. I am completely open to whether restructuring will aid that, and I look forward to sitting down with the commissioners—I am going to do it this week—to have a discussion about their recommendations. I am open to it. More has to be done. I think we have made strides, but we still have a ways to go. And they point out areas which we have not gone as far as any of us would like.

So I look forward to not only talking with the commissioners, but also spending time with the Attorney General to determine whether any restructuring, how that would fit in with what is happening in the Department of Justice, because it is the two of us working together.

Chairman SPECTER. Director Mueller—

Director MUELLER. And DNI, if I might say. The relationship with the DNI is particularly important and I want to have an opportunity to sit down with the DNI and look at how the restructuring proposed might assist him and his responsibilities.

Chairman SPECTER. Well, the restructuring is fine, but it is going to take a lot more coordination. This is something that you and I are going to talk about in greater length after today's hearings and will be a very important provision for this Committee's oversight.

When I finished my last round, I was on a fellow known as Curveball, and it was rather obtuse as to—but I wanted to end on time, which I think is important to keep this hearing moving. But just by way of slight amplification, Curveball was supposed to have been the name for an informant who gave information which was relied upon that Iraq had weapons of mass destruction. And there were serious challenges to Curveball's veracity and, in a surprising way, both former Director Tenet at the CIA has been quoted as saying he never heard of Curveball and, similarly, Deputy Director McLaughlin has been quoted as saying that he never heard of Curveball. And those are questions which really need to be answered on the record, aside from simply the newspaper accounts.

But so often we find that this sort of thing occurs just sort of incomprehensible when major decisions are made and the matters do not get to the upper echelons. It places a very heavy burden on the Attorney General and on the Director. But as those questions were asked about the questioning at Guantanamo, it really is something that has to get to the upper echelons because, regrettably, if it does not, the action simply is not taken.

There are a couple of other questions I want to come to before concluding the hearing. When we were talking about tangible things, Attorney General Gonzales, talking about probable cause as opposed to relevance and Senator Durbin raised the question about whether the Judiciary Committee got information, we are going to

seek a memorandum of understanding that now goes to the Intelligence Committee. But would there be a major burden if probable cause were used as opposed to the standard of relevance? As Senator Durbin pointed out, once you have relevance, there is a "shall" requirement that the judge issue the search and seizure warrant. How big a burden would it be if the traditional standard of probable cause were used here?

Attorney General GONZALES. Well, Mr. Chairman, I think that probable cause is appropriate in connection with searches and seizures. When we are talking about provisions such as 215, that is not a search in the traditional sense. That represents simply obtaining information from a third party, where there is less, I think, expectation of privacy. And information is gathered—this is the way it happens in criminal cases. You use grand jury subpoenas to gather information using relevancy standards, and then once you gather—it is a building block, and once you gather the information, then you use that to conduct your searches and seizures. And so I am told by our agents and the prosecutors that if we were to elevate, for example, the standard with respect to 215 from relevance to probable cause, no one would use 215. And I just think it is an important tool, that we ought to make it a viable tool, and I am concerned that if in fact the standard were raised, that would not be the case.

Chairman SPECTER. Attorney General Gonzales, in your answer I heard you use the term "search and seizure" after you said it was not a search and seizure. It seems to me it is a search, going after a specific record; and then a seizure to obtain it.

We are going to have a closed-door session on the 12th, a week from today, and I am going to want to hear specifics. I like to function on a fact-oriented basis.

Attorney General GONZALES. As do I, Senator.

Chairman SPECTER. I want to hear specifics where there have been obtaining the records under a tangible-things Section 215, and specifically why there would be a problem on probable cause. My own experience has been that if you stop and think for a few minutes, you have a reason as to why you want it. Probable cause does not have to be some elaborate statement of an affidavit in the search warrant, it has to be the reason you are looking for. And there usually—if there is justification, I think the law enforcement officer can articulate a reason. But I want to come down to the specifics when we are in a closed-door session.

Similarly, Director Mueller, when we talk about the search-and-peek, you gave one illustration as to the provision 5 on catch-all. I want to hear more about it. As I cited to you, some—

Director MUELLER. Ninety-two. I think it was 92—

Chairman SPECTER. Twenty-eight matters where they were solely on the basis of that exception. And here again, I would like to hear the specifics as to why they do not fall into a specific category.

And on the multi-point wiretaps, where you have the non-specification of an individual, as Senator Feinstein talked about, the John Doe wiretaps, and you have multi-points, it seems that it is really generalized. And there are 49 of these applications made—and here again, I want to get into the specifics as to exactly what they are.

Our Committee has been looking at possible legislation on an expansion of the authority of the FISA court to be the central court where applications are made for habeas corpus on detention. We now have conflicting decisions by the district courts. I would be interested in your views, Attorney General Gonzales, if you think that would be helpful to have that concentrated in one court so you have uniform application.

We are also thinking about spelling out some of the—in more detail. It is congressional authority under the Constitution to deal with this issue of detentions, but what, do you think it useful from the point of view of the Department of Justice if there was a central court, to avoid the question of conflicting decisions?

Attorney General GONZALES. I think it could certainly be useful, Mr. Chairman. Obviously, we would like the opportunity to look at the legislation.

Chairman SPECTER. Well, you will have a chance to look at the legislation. How about you, Director Mueller? How about disagreeing with the Attorney General for once here today?

Director MUELLER. I disagree with the Attorney General. I do not think that—

No. I have not had a chance to think about whether a central court in that circumstance would make a difference. I would like to get back to you on that.

Chairman SPECTER. Attorney General Gonzales did not have a chance to think about it, either, but he had an answer.

Attorney General GONZALES. I said I thought it could be helpful.

Chairman SPECTER. We are going to be having another hearing on the PATRIOT Act on May 10. We have started early. This is a big issue.

I was about to conclude the hearing until my peripheral vision was a little too good to see Senator Schumer return. Senator Schumer, you do not have any more questions, do you?

Senator SCHUMER. Just one, very brief, Mr. Chairman.

Chairman SPECTER. Proceed in that event.

Senator SCHUMER. Thank you. And I appreciate it and apologize for coming back and forth to the witnesses and to you. We have three different committees going.

Chairman SPECTER. Oh, it is quite all right, we know you are busy. Especially since you promised only one question.

Senator SCHUMER. Exactly.

This is to Director Mueller. It has several parts, as the Chairman knows.

[Laughter.]

Director MUELLER. Somehow I am not surprised.

Chairman SPECTER. Director Mueller, he can ask you as many parts as he wants. You only have to give one answer.

Senator SCHUMER. With many parts.

Anyway, Director, I know that you, in response to a letter that I, along with Senator Lautenberg and others, sent—this is just to follow up on the guns issue that I had asked about before—have formed a working group to review this problem. When can we expect to hear from the working group in terms of a real time frame?

That is my only question.

Director MUELLER. It is a Justice Department working group under the Attorney General, sir.

Senator SCHUMER. Ah. Excuse me.

Director MUELLER. So for once I will defer to the Attorney General.

Senator SCHUMER. Then let me—

Attorney General GONZALES. Senator Schumer, I do not have an answer, but I will respond to you shortly as to when we will have a report.

Senator SCHUMER. What, is it going to take a very long time, or are we going to get back before the PATRIOT Act comes before us?

Chairman SPECTER. You are on your second question, Senator Schumer.

Senator SCHUMER. Well, that was a follow-up question. You are a good attorney, better than me. Follow-up questions.

Attorney General GONZALES. I would hope it would not take a long time, but I need to check with my staff, Senator.

Senator SCHUMER. Okay. Could we get an answer back in writing as to when it would—when we would get the answer?

Attorney General GONZALES. We will do our best, Senator.

Senator SCHUMER. Thank you.

Mr. Chairman, was a I brief enough?

Chairman SPECTER. I consider those three questions all within the ambit of the single question.

Let me thank you on behalf of the Committee, Attorney General Gonzales and Director Mueller, for the service you perform. Attorney General Gonzales spent 4 years as White House Counsel—and you have had a very distinguished career. I think Senator Sessions was right, a little undue modesty in terms of your long tenure as U.S. attorney both in Boston and San Francisco, assistant attorney general. And these are very knotty problems and I am glad to see some showing of flexibility. I think there has to be a little give on some of these issues. And as I say, when we have the closed-door session, I want to see the specifics. I want to see exactly what is going on and how we might leave you the authority you need but still have the specifications so that the standards are interpretable by people down the line to protect civil rights.

I would like to see both of you gentlemen in the back room, if I might, for just a minute.

That concludes the hearing.

[Whereupon, at 12:47 p.m., the hearing was concluded.]

[Questions and answers and submissions for the record follow.]

[Additional material is being retained in the Committee files.]

QUESTIONS AND ANSWERS



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

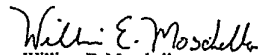
Dear Mr. Chairman:

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 5<sup>th</sup> 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. Lasaun 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 OCDETF 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 comprise 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 BIA 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 108<sup>th</sup> 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 NSLs under these statutory provisions.

Information regarding NSLs, including the number of requests made pursuant to these authorities, is classified. However, as required by statute, the use of NSL 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 OIFR, 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 study currently 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 a 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 am 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).

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 93  
Page 96 ~ Outside the Scope  
Page 97 ~ Outside the Scope  
Page 98 ~ Outside the Scope  
Page 99 ~ Outside the Scope  
Page 100 ~ Outside the Scope  
Page 101 ~ Outside the Scope  
Page 102 ~ Outside the Scope  
Page 103 ~ Outside the Scope  
Page 104 ~ Outside the Scope  
Page 105 ~ Outside the Scope  
Page 106 ~ Outside the Scope  
Page 107 ~ Outside the Scope  
Page 108 ~ Outside the Scope  
Page 109 ~ Outside the Scope  
Page 110 ~ Outside the Scope  
Page 111 ~ Outside the Scope  
Page 112 ~ Outside the Scope  
Page 113 ~ Outside the Scope  
Page 114 ~ Outside the Scope  
Page 115 ~ Outside the Scope  
Page 116 ~ Outside the Scope  
Page 117 ~ Outside the Scope  
Page 118 ~ Outside the Scope  
Page 119 ~ Outside the Scope  
Page 120 ~ Outside the Scope  
Page 121 ~ Outside the Scope  
Page 122 ~ Outside the Scope  
Page 123 ~ Outside the Scope  
Page 124 ~ Outside the Scope  
Page 125 ~ Outside the Scope  
Page 126 ~ Outside the Scope  
Page 127 ~ Outside the Scope  
Page 128 ~ Outside the Scope  
Page 129 ~ Outside the Scope  
Page 130 ~ Outside the Scope  
Page 131 ~ Outside the Scope  
Page 132 ~ Outside the Scope  
Page 133 ~ Outside the Scope  
Page 134 ~ Outside the Scope  
Page 135 ~ Outside the Scope  
Page 136 ~ Outside the Scope  
Page 137 ~ Outside the Scope  
Page 138 ~ Outside the Scope  
Page 139 ~ Outside the Scope

Page 140 ~ Outside the Scope  
Page 141 ~ Outside the Scope  
Page 142 ~ Outside the Scope  
Page 143 ~ Outside the Scope  
Page 144 ~ Outside the Scope  
Page 145 ~ Outside the Scope  
Page 146 ~ Outside the Scope  
Page 147 ~ Outside the Scope  
Page 148 ~ Outside the Scope  
Page 149 ~ Outside the Scope  
Page 150 ~ Outside the Scope  
Page 151 ~ Outside the Scope  
Page 152 ~ Outside the Scope  
Page 153 ~ Outside the Scope  
Page 154 ~ Outside the Scope  
Page 158 ~ Outside the Scope  
Page 159 ~ Outside the Scope  
Page 160 ~ Outside the Scope  
Page 161 ~ Outside the Scope  
Page 162 ~ Outside the Scope  
Page 163 ~ Outside the Scope  
Page 164 ~ Outside the Scope  
Page 166 ~ Outside the Scope  
Page 167 ~ Outside the Scope  
Page 168 ~ Outside the Scope  
Page 169 ~ Outside the Scope  
Page 170 ~ Outside the Scope  
Page 171 ~ Outside the Scope  
Page 172 ~ Outside the Scope  
Page 173 ~ Outside the Scope  
Page 174 ~ Outside the Scope  
Page 175 ~ Outside the Scope  
Page 176 ~ Outside the Scope  
Page 177 ~ Outside the Scope  
Page 178 ~ Outside the Scope  
Page 179 ~ Outside the Scope  
Page 180 ~ Outside the Scope  
Page 181 ~ Duplicate  
Page 182 ~ Duplicate  
Page 183 ~ Duplicate  
Page 184 ~ Duplicate  
Page 185 ~ Outside the Scope  
Page 186 ~ Outside the Scope  
Page 187 ~ Outside the Scope  
Page 188 ~ Outside the Scope  
Page 189 ~ Outside the Scope  
Page 190 ~ Outside the Scope  
Page 191 ~ Outside the Scope  
Page 192 ~ Outside the Scope