S. HRG. 110–881

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 27, 2007

Serial No. J–110–23

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

38–189 PDF WASHINGTON : 2009

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island

ARLEN SPECTER, Pennsylvania
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts, prepared statement	156
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	158
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania	3

WITNESS

Mueller, Robert S., III., Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C.	5

QUESTIONS AND ANSWERS

Responses of Robert S. Mueller to questions submitted by Senators Leahy, Kennedy, Biden, Schumer, Specter and Grassley	45

SUBMISSIONS FOR THE RECORD

Coalition of Civil Rights, Education, Religious, Professional, and Civic Organzation:	
June 26, 2006, letter	122
October 23, 2006, letter	128
Department of Justice:	
Federal Bureau of Investigation, Criminal Justice Information Services Division, Thomas E. Bush, III, Assistant Director, letter	131
Office of Legislative Affairs, William E. Moschella, Assistant Attorney General, letter	133
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa:	
March 22, 2007, letter	143
March 26, 2007, letter	145
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, letter	161
Mueller, Robert S., III., Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement	163
Washington Post, John Solomon, Staff writer, March 27, 2007, article	178

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

TUESDAY, MARCH 27, 2007

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC

The Committee met, pursuant to notice, at 9:37 a.m., in room 106, Dirksen Senate Office Building, Hon. Patrick J. Leahy, (Chairman of the Committee) presiding.

Also present: Senators Feinstein, Feingold, Schumer, Durbin, Cardin, Whitehouse, Specter, Hatch, Grassley, Kyl, Sessions, and Cornyn.

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

Chairman LEAHY. Good morning. We are continuing our crucial oversight role of the Department of Justice with this hearing to examine the FBI's effectiveness in carrying out its domestic intelligence and law enforcement mission.

I thank the FBI Director for appearing before us today. I look forward to hearing his views on the Bureau's problems and progress. I also thank the hardworking men and women of the FBI who have been working long hours, day in and day out, all week long, year after year, to keep our citizens and our communities safe.

Almost 6 years after the September 11th attacks, it troubles all of us that the FBI has not yet lived up to its promise to be the world-class domestic intelligence agency the American people expect and need it to be.

This morning we learn from a report in the Washington Post that the FBI has repeatedly submitted inaccurate information to the Foreign Intelligence Surveillance Court in its efforts to obtain secret warrants in terrorism and espionage cases, severely undermining the government's credibility in the eyes of the Chief Judge of that court.

When I read that last night online, they were talking about even considering making people who sent these reports in come in and appear under oath. That is a very problematical thing, and it bothers me very much.

But from the FBI's illegal and improper use of National Security Letters, to the Bureau's failure to be accountable for securing its own computers and weapons, to the politically motivated dismissal of eight of the Nation's U.S. Attorneys, there are growing concerns

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

about the competence of the FBI and the independence of the Department of Justice.

This pattern of abuse of authority and mismanagement causes me and many others on both sides of the aisle to wonder whether the FBI and Department of Justice have been faithful trustees of the great trust that the Congress and American people have placed in them to keep our Nation safe, while respecting the privacy rights and civil liberties of all Americans.

It is more than just the FBI that deserves scrutiny for the abuses and lack of competence that have come to light in recent weeks. Last year, the administration sought new powers in the Patriot Act to appoint U.S. Attorneys without Senate confirmation, and new powers to more freely use National Security Letters. The administration got these powers and they bungled both of them.

One of my priorities in the first Patriot Act was to improve oversight and accountability. Former House Majority Leader Dick Armey and I insisted on, and succeeded in, adding sunset provisions to the Patriot Act which would require us to review what was going on.

In the recent reauthorization of the Act, one of my priorities, working especially with then-Chairman Specter, was to retain sunset provisions, and add new sunshine provisions to require the Justice Department to report to the Congress and the American people on how several parts of the Act are being used.

The Inspector General's audit and report on National Security Letters was one of these new requirements we added to the law. The findings of that audit were very troubling findings, and why we are here today.

I am deeply disturbed by the Justice Department Inspector General's report finding widespread illegal and improper use of National Security Letters to obtain Americans' phone and financial records. Let me underscore that: widespread illegal and improper use.

The Inspector General found 22 separate instances where the FBI improperly abused National Security Letters. In case you think 22 does not seem like a lot, that is 22 in a review of only 77 files, and not a single one of those violations had been reported by the FBI.

When he appeared before Congress last week, the Inspector General testified there could be thousands of additional violations among the tens of thousands of NSLs that the FBI is now using each year.

Inspector General Fine also found widespread use by the FBI of so-called "exigent" letters. These letters, which are not authorized by any law, were used 739 times to obtain Americans' phone records. But there was often no emergency, and never follow-up subpoenas promised in the letter.

Despite these extensive abuses, the top leadership of the FBI sat idly by for years doing nothing to stop this practice. In fact, the Washington Post recently reported the FBI counterterrorism officials continue to use the exigent letters, even though FBI lawyers and managers expressed reservations as early as 2004.

So I have already told the Director I want to hear what he has to say about this and what the FBI is doing to ensure these abuses will not happen again.

I look forward to exploring the Bureau's failure to account for its laptop computers and weapons, delays with the Sentinel computer program, staffing shortages, and growing calls to replace the Bureau's Counterterrorism and Counterintelligence divisions with an MI–5-style domestic intelligence agency.

It seems to me the FBI is, again, at a crossroads. Some are calling on Congress to take away the FBI's domestic intelligence functions and create a separate domestic intelligence like Britain's MI–5. The leading Republican on this oversight Committee questioned whether the Director is up to the job.

Acknowledging shortcomings is well and good, and Director Mueller, in what seems to be a break from many in this administration, now says that he takes responsibility for the egregious violations that occurred during the handling of the NSLs, as he should.

But the Bureau, and the Department as a whole, must also learn from its mistakes if progress is to be made, and the Congress has a right to ask about that. This learning curve has gone on far too long. A lot needs to be done. I want the FBI to be the best that it can be, and I hope our oversight might make that possible. We have a long way to go.

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

Senator Specter.

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

Senator SPECTER. Thank you, Mr. Chairman.

The war against terrorism is deadly serious, and we know, in retrospect, that 9/11 could have been prevented had there been adequate intelligence and adequate coordination among our intelligence agencies.

The United States places great reliance on the FBI and it has an illustrious history. But the question is emerging as to whether the FBI is up to the enormous task that we have asked it to perform. Every time we turn around, there is another very serious failures on the part of the Bureau.

We had the Inspector General in last week and went over three of the Inspector General's reports, and they present a picture of lack of competence, to put it mildly.

On the National Security Letters, the Inspector General found "widespread and serious misuse of the FBI's National Security Letter authorities. The oversight was inconsistent and insufficient."

Then within the past 45 days, in a report on the issue of terrorism reporting, the Inspector General concluded, "the collection reporting of terrorism-related statistics within the Department is haphazard."

Then on the issue of weapons and laptops, "the FBI could not determine, in many cases, whether the lost or stolen laptop computers contained sensitive or classified information."

Then another shoe drops, virtually on a daily basis. The headline in this morning's Post: "FBI Provided Inaccurate Data for Surveillance Warrants," and the Foreign Intelligence Surveillance Court threatened to require affidavits in open court, and a real question as to whether the FBI was performing so they could get warrants, as required under the law, to fight terrorism.

With respect to the National Security Letters, the Inspector General's report found that the FBI agents consistently signed exigent letters where they had no exigent circumstances, and it went on repeatedly without any correction.

The Inspector General said that there was no evidence of intentional misconduct, but where you have that pattern of reckless indifference, at a minimum, that rises to the level of what constitutes intentional misconduct. So, these are all matters of enormous concern.

Director Mueller, this Committee has enormous respect for you, and I have enormous personal respect for you. The question arises as to whether any Director can handle this job. The further question arises as to whether the Bureau itself can handle the job.

These instances have stimulated recent debate on whether we ought to turn to the British MI–5 system. I believe, Mr. Chairman, that that is a consideration which would warrant very serious deliberation by this committee. We have authorities lined up on both sides, but there are sufficient problems that I think it needs to be considered.

We had recent reports with respect to the termination of U.S. Attorney Lam in San Diego, that there may have been a request for her resignation because she was hot on the pursuit of other leads following the conviction of former Congressman Duke Cunningham and the 8-year prison sentence which he is now serving.

I know in the San Diego Union Tribune there were comments by the FBI's San Diego office head that her termination was jeopardizing several ongoing investigations, and he used the word "guaranteed" in referring to politics being involved.

If this is so, Mr. Director, this is not something that the Justice Department ought to read about in the newspapers. If there is any indication that Ms. Lam was asked to resign because she was hot on the trail of other political operatives on the issue of corruption, as with the Cunningham case, I would suggest to you that the FBI has an affirmative duty to, at a minimum, come to the Chairman and Ranking Member to report matters of that sort. So, there are a great many issues which we have to take up.

It may be that the Congress and the administration are not providing sufficient resources to the Bureau. I appreciated an opportunity yesterday afternoon, Director Mueller, to talk to you personally and directly on these issues. I believe that there has to be more attention paid to the issues as to whether we are asking more of you than the available resources would permit you to perform on.

When we talked about successes that the FBI has had on terrorism matters, where you have successes and you cannot publicize them, as I mentioned to you yesterday, I would call on you to come in and talk to Senator Leahy and myself about those matters.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Mr. Director, would you please stand and raise your right hand?

[Whereupon, the witness was duly sworn.]

Chairman LEAHY. Director, please go ahead with your statement. I am going to ask members to keep as close to their time in questioning, and you in your statement, as possible because we have a number of matters going on, other Committee meetings, and I want as many Senators as possible to have a chance to ask questions.

Please go ahead, sir.

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, Senator Specter, and Members of the Committee, thank you for the opportunity to testify before you today.

For the past five and a half years, the FBI has been undergoing significant restructuring, significant realignment, and significant transformation, all designed to better position the Bureau to meet the threats and the challenges of the future. The men and women of the FBI have demonstrated the ability and the willingness to embrace change for a better, stronger, more effective organization.

As a result of these changes and the dedication of FBI employees, our accomplishments have been many. They include: terrorist plots thwarted, espionage activities intercepted, cyber-intrusions detected, corrupt government officials convicted, violent gangs dismantled, and corporate fraud uncovered. Examples of these successes were provided to the Committee when I last testified here in December.

Now, many of our counterterrorism cases have included the issuance of National Security Letters. Today, given the recent Inspector General report, I would like to address our use of those letters.

The Inspector General and his staff conducted a thorough and a fair review of this authority, and the Congress is commended for requiring that this review be conducted. It is absolutely effective and appropriate oversight.

And as you heard from the Inspector General, he did not find any deliberate or intentional misuse of National Security Letter authorities, Attorney General guidelines, or FBI policy.

And with regard to the use of exigent letters before this committee, he testified that he did not find an intent to violate the law, but rather "the unthinking use of improper form."

Nevertheless, the review by the Inspector General identified several areas of inadequate auditing and oversight of these vital investigative tools, as well as processes that were inappropriate.

We in the FBI, myself in particular, fell short in our obligations to report to Congress on the frequency with which we use this tool and in the internal controls we put into place to make sure that it was used only in accordance with the letter of the law. I am responsible for those shortcomings, and I am also responsible for taking the steps to ensure that they do not happen again.

The IG made 10 recommendations designed to provide both the necessary controls for the issuance of NSLs and the creation and

maintenance of accurate records. I fully support each recommendation and I am taking steps to implement them, as well as a number of other steps that will ensure that we are in compliance with applicable statutes and guidelines.

No one in the FBI wants to jeopardize the important tools that Congress has provided to us to protect the country against a terrorist attack. Mr. Chairman, my prepared statement provides a thorough review of the three major findings by the Attorney General—or by the Inspector General, I should say, and also explains the steps that we are taking to address each of these shortcomings.

I am very happy to provide additional detail in response to questions that the Committee may have, but for the purposes of my remarks this morning I would like to provide the general contexts surrounding the FBI's use of National Security Letters, as well as a couple of examples of how essential these tools are in combatting terrorism.

As this Committee is well aware, the FBI began a significant transformation following the terrorist attacks of September 11. In the aftermath of that date, the men and women of the FBI understood that counterterrorism is our first priority and that every counterterrorism lead must be addressed.

As Congress was providing us with new authorities in support of this mission, we were also undergoing substantial overhaul of our counterterrorism program.

By way of an example, we established a number of operational entities, including the 24/7 Counterterrorism Watch, the National Joint Terrorism Task Force, Terrorist Screening Center, Terrorist Financing Operation Section, and rapid deployment teams.

We expanded our intelligence capabilities, elevating intelligence to a program level status and putting in place a Directorate of Intelligence to govern FBI-wide intelligence functions and establishing field intelligence groups in every field office.

We enhanced our information sharing with our partners by expanding our Joint Terrorism Task Forces, increasing technological connectivity, and developing new vehicles for communications, such as the Intelligence Bulletin.

We replaced outdated computer hardware with more than 30,000 new desktop computers with modern software applications, and deployed a high-speed secure network, enabling personnel in FBI offices across the country and around the world to share data, including audio, video, and image files.

As these reforms were being implemented, the men and women of the FBI were also charged with protecting this Nation from terrorist threats of unprecedented dimensions.

While I am unable to provide a full picture of the nature of these threats in such a public hearing, some of the plots investigated and thwarted include destruction of the New York Stock Exchange and other financial targets; attacks on U.S. military facilities, Israeli government facilities, and Jewish synagogues in the Los Angeles area; the destruction of the Brooklyn Bridge in New York City; and the explosion of commercial aircraft as they traveled from London to United States destinations, to name a few.

In addition to these threats which have been publicly reported, a number of other plots were being addressed for which the mas-

termind of September 11th, Khalid Sheik Mohammad, has recently claimed credit. Those details remain classified.

Mr. Chairman, it is within this environment of significant internal transformation and unprecedented worldwide terrorist threats that the FBI was utilizing the important new authorities that Congress had provided in the USA Patriot Act.

I do not offer this explanation as an excuse for any of the shortcomings found by the Inspector General, but only to provide an over-arching context for the Committee and the American people. Even within this context, mistakes made with regard to National Security Letters are simply not acceptable.

As explained in detail in my prepared statement, these deficiencies are being addressed and I welcome the committee's input and suggestions for additional improvements to our internal controls.

I do not believe, however, that the statute itself should be changed. The relevant standard established by the Patriot Act for the issuance of National Security Letters is unrelated to the problems identified by the Inspector General.

As the Inspector General testified, the problems were generally the product of "mistakes, carelessness, confusion, sloppiness, lack of training, lack of adequate guidance, and lack of adequate oversight." In short, the statute did not cause the errors, the FBI's implementation of the statute did.

In the meantime, I do believe it is important that the Congress and the American people understand how essential National Security Letters are to our efforts in the war on terror.

A couple of examples. During the investigation of a terrorist financier and recruiter, the FBI issued National Security Letters for financial records and telephone toll billing records. These records helped the FBI identify banks and accounts that were being used to facilitate his terrorist fundraising efforts.

He eventually was identified by someone as an individual who would provide instructions for terrorist activities in the United States, and although this financier and recruiter was not prosecuted, he was deported based upon the information developed during the investigation and attributable to the information received by National Security Letters.

Another case. Last year, the FBI received information from a foreign government indicating that persons using e-mail addresses in the United States were in contact with an e-mail address belonging to a suspected terrorist.

The FBI served NSLs on the relevant Internet service providers, and the investigation which followed indicated that these individuals were involved in plots against the United States, resulting in indictments on various terrorism-related charges.

Chairman LEAHY. Director Mueller, we could go into a number of these NSLs, a number of them that I've looked at. We're not going to in an open session. We can talk about how some have differing views of how serious a plot it was to take down the Brooklyn Bridge, and others.

I'm not so much interested in those statistics. Remember, I, along with Senator Specter, have supported the idea of the NSLs.

I also expect them to be used right, because the ability to abuse them is enormous.

Let me—

Director MUELLER. May I finish my statement, Mr. Chairman? It is very short. I have a few minutes left.

Chairman LEAHY. I think we are a little bit over time, but go ahead, finish it.

Director MUELLER. Thank you. Let me conclude on this by saying, as reflected in these examples, through NSLs the Bureau has established financial and e-mail linkages that resulted in further appropriate investigation.

As the Inspector General has so testified, NSLs are an indispensable—indispensable—tool in our conduct of counterterrorism and counterintelligence investigations.

Now, for a moment, Mr. Chairman, I would like to turn to a couple of other issues that I know are on the committee's mind. The first, is the deployment of Phase I of Sentinel. As your staff has recently been briefed, our contractor, Lockheed Martin, has completed the critical design and build of the software application and is presently in the testing phase.

Once testing is complete sometime next month, we will begin piloting Phase I at Headquarters, followed by several field offices, during which time Lockheed Martin will correct any additional issues that surface.

Shortly after that, shortly after we complete the testing in the pilot offices, we will begin a roll-out of Sentinel throughout our organization. Again, we will continue to keep the Committee updated on our progress in the weeks ahead.

I would also like to note, in addition to counterterrorism, counterintelligence, and cyber responsibilities, public corruption remains our top criminal investigative priority.

Public corruption is a betrayal of the public's trust and cannot be left unchecked. Over the last 2 years, the FBI has convicted more than 1,000 government employees involved in corrupt activities, to include 177 Federal officials, 158 State officials, and 360 local officials, as well as more than 365 police officers.

Finally, as this Committee is aware, the country is experiencing an uptick in violent crime, particularly as it relates to gang violence. By our estimates, there are now over 30,000 gangs across America and over 800,000 gang members.

As with terrorism, the most powerful response to this growing problem is a joint response. The FBI has established 131 violent gang task forces across the country, enabling our agents to work in lock step with police on the street, sharing information and conducting investigations together.

And while our number-one priority remains preventing another terrorist attack, the FBI remains committed to working with our partners to combat violent crime and to lower crime rates across America.

In closing, Mr. Chairman, let me reiterate that the FBI is acutely aware that we cannot protect against national security or criminal threats at the expense of civil liberties. We are judged not just by our ability to defend the Nation from attacks, but also our commitment to defend the rights and freedoms we all enjoy.

In light of the Inspector General's findings, we are committed to demonstrating to this committee, to the Congress, and to the American people that we will correct the deficiencies in our use of National Security Letters and utilize each of the critical tools Congress has provided us, consistent with the privacy protections and civil liberties that we are sworn to uphold.

Thank you for the opportunity to conclude my statement, and I am happy to answer any questions you might have, sir.

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

Chairman LEAHY. Well, I do have a few. I must admit that when I've listened and read your statement, I still have some very serious qualms. You said there's an uptick in violent crimes. The administration—it's not your decision, but the administration decision to cut money for COPS grants and other things, apparently because we need the money to pay for the well-run police forces of Iraq.

The Federal Government has spent almost $200 million on the long-promised Integrated Wireless Network. Now we find the Justice Department spent $772 million on that. The Department of Justice and DHS, Department of Homeland Security, can't seem to get together.

It's almost like one of you are the Sunnis and the others are the Shi'ites, and somebody's got to tell the people—somebody in the administration ought to at least admit some mistakes and tell you guys that we're all supposed to be Americans. We're all supposed to be working together. And I know you have your own frustrations, and we can go into it later.

We talk about the ability to obtain library records under the PATRIOT Act. That gives me some concern, and I'll tell you why. I'll just use an example. In 2005, the FBI issued National Security Letters to four Windsor, Connecticut librarians.

Here's what they asked them to do: surrender all subscriber information, billing information, and access logs of any person related to a specific library computer during a specific time period, according to press reports. But then the NSL also prohibited the librarians from disclosing the fact that they received the NSL or its contents, a so-called gag order, under the PATRIOT Act.

So what you have is, if somebody sees a real abuse of an NSL, it's like saying, let's check the records of everybody who showed up in this hearing today, every citizen who showed up as a member of the press or anybody else who came to this, but let's not tell anybody we've done it. If there's abuses, the very people who could uncover those abuses have been gagged, told they can't say what's going on. This is Kafka at the extreme.

Did the FBI abuse—two questions. Did the FBI abuse its authority in this Connecticut case? And how many times has the FBI issued NSLs to libraries or educational institutions to date?

Director MUELLER. A couple things, Mr. Chairman. The PATRIOT Act was changed in the most recent iteration to provide an opportunity for somebody to context portions of—

Chairman LEAHY. In this case, did the FBI abuse its authority?

Director MUELLER. I do not believe so. But let me—

Chairman LEAHY. How many times have you issued NSLs to libraries or educational institutions to date?

Director MUELLER. I cannot think of one, but I'll have to go back and check. And I also—

Chairman LEAHY. Was this Connecticut library the only one?

Director MUELLER. I will have to go back and check.

Chairman LEAHY. Will you supply the answer? Can we get that answer before the end of the week?

Director MUELLER. Yes. May I also say, Mr. Chairman, that there was a report on our use of 215 of the PATRIOT Act that was issued by the Inspector General on the same day he issued the report with regard to our use of National Security Letters.

That report found no abuse and appropriate use of the 215 authority. It did not get much press, it did not get much attention, but it also discusses our use of Section 215 with regard to libraries. But again, I'd reiterate, that report that came out the same day as the report on NSLs found our appropriate utility of Section 215 of the PATRIOT Act.

Chairman LEAHY. Over the weekend, the Justice Department announced that the Office of the Inspector General and the Office of Public Integrity have launched a joint investigation into the firing of the eight U.S. Attorneys, something this Committee is doing also.

Is the FBI investigating the allegations that have come to light about politically motivated firings of eight of the Nation's U.S. Attorneys?

Director MUELLER. No.

Chairman LEAHY. Have you been asked in any way to join with the Office of Inspector General or the Office of Public Integrity in these investigations?

Director MUELLER. Not to my knowledge. In other words, I have not personally. I don't believe anybody in our organization has either.

Chairman LEAHY. Will you check that—

Director MUELLER. I will check that.

Chairman LEAHY.—and let me know this week?

Director MUELLER. Yes, sir.

Chairman LEAHY. Thank you.

We talked a lot about the use of the NSLs, the Inspector General's reports. You've spoken about your own responsibility. I realize, though, this is a very large organization. We're going to be reexamining the broad authorities we've granted to the FBI under the PATRIOT Act, but in the meantime I just want to ask what's being done in your shop.

I mentioned the 739 so-called exigent National Security Letters, even though there's no emergency in some of these cases. The FBI also sent these NSLs without issuing a subpoena. It said, of course, the subpoena would be forthcoming. Just put yourself in the position, for example, of the phone company, or something.

They come in and the agent hands them that. They actually have a department for that. They hand them the letter and they say, but don't worry. Don't worry. There's going to be a subpoena, but we need this right now. Now, their general counsel is going to say, of

course, follow that and make sure you get the subpoena. But then we find the subpoenas never showed up.

Today we learned through the press—not from anything we were told by the Department of Justice, we learned from the press, just as time and time and time again, even though we have these oversight hearings, we first hear about these things from the press, that the FBI repeatedly submitted FISA applications with inaccurate information to the Foreign Intelligence Surveillance Court to obtain secret warrants on terrorism and espionage cases.

We set up all these procedures to help you, but we assume somebody is going to follow the rules. What kind of management failures made it possible for the FBI to send out hundreds of National Security Letters containing significant false statements about forthcoming subpoenas?

Director MUELLER. Let me start by answering the first part of the question, what we are doing about it. We have, in the areas of concern identified by the Inspector General with regard to the numbers, we have changed our procedures on the numbers—identifying the numbers of National Security Letters. We are requiring a hand count every month. We are keeping copies of each National Security Letter in separate files.

Chairman LEAHY. Had you been alerted of these abuses back in 2004 when they were first discovered?

Director MUELLER. No. But—

Chairman LEAHY. Is that a failure of management?

Director MUELLER. Yes.

Chairman LEAHY. Okay.

Director MUELLER. With regard to the future, we have a software package and a computer program we started developing last spring that will go online later this year that will assure that every NSL is recorded and the appropriate information is recorded for every NSL.

We have gone back and done, over the last several weeks, a follow-up audit on IOB—possible IOB violations where we've had more than 150 inspectors at each of our offices doing a 10 percent audit to follow-up.

Chairman LEAHY. And going back to that, are you finding information that was obtained, that it was unlawfully obtained?

Director MUELLER. We're still getting the results of that review, and there will be additional—I would expect additional field work before we come to any conclusions.

Chairman LEAHY. Have you seen any information that was unlawfully obtained?

Director MUELLER. Not so far. But I would expect there to be some because I would expect, in the course of those audits, that they would have found IOB violations that had not been reported, or NSLs that had not been reported.

So I assume and presume in those results that there will be additional instances. We are going to do a periodic review with the Department of Justice of our various offices, up to 15 this year, where we go in in-depth.

Those are just to mention a couple of the areas in which we are addressing this issue. But it's more fundamental than that, and it goes back to the question of, how could this have happened?

And the way it happened was that we, in the wake of the national security letters, when we got the authority, we put into place procedures to account for NSLs. We put into place procedures that the numbers would be recorded by the Office of General Counsel.

We put into place procedures that we thought would be followed in terms of giving us the accurate numbers and accurate possible IOB violations. What I did not do, and should have done, is put in a compliance program, complete with auditing and follow-through to assure that those procedures were being followed. That is something I should have recognized. It's something I should have put into place before, and it is something we are developing not just for NSLs, but across the board, a compliance program.

I will tell you, Mr. Chairman, that when giving us funds, Congress does not look at separate funding for compliance programs. They give us funds to address terrorism, they give us funds to address gangs, give us funds to address the criminal challenges we have. For me, I have to focus on the fact that we need funding for compliance programs.

We need funding for additional lawyers, we need to put into case—into place the auditing capabilities that would show and point out the deficiencies, such as we found in this Inspector General's report.

Chairman LEAHY. My time is up. When we come back I may talk about how the administration spends funds on law enforcement in Iraq. They ought to spend some back here at home.

Director MUELLER. Sure.

Chairman LEAHY. Senator Specter.

Senator SPECTER. Director Mueller, does the FBI have sufficient funding on intelligence and counterintelligence matters to protect the Nation from another terrorist attack?

Director MUELLER. We have requested funds that we have not received, whether it be through the Department of Justice or through the budget process. So there are items we need and would want that would—that would enhance our ability to protect the American public.

Senator SPECTER. How much additional funding does the FBI need on intelligence and counterintelligence matters to protect the Nation from another terrorist attack?

Director MUELLER. I would hate to give you off the—I will provide that information.

Senator SPECTER. Would you please provide that?

Director MUELLER. Yes, sir.

Senator SPECTER. Because we're asking you to do many, many things, and the most important thing we're asking you to do is to protect America from another terrorist attack. And this committee, the Congress, would like to know what funding you need to do that.

Turning to another subject, the San Diego Union Tribune has this part of the story on January 13 of this year: "The FBI chief said Lam's continued employment as U.S. Attorney is crucial to the success of multiple ongoing investigations."

Director Mueller, is it true that Lam's continued employment as U.S. Attorney was crucial to the success of multiple ongoing investigations?

Director MUELLER. I don't believe that to be the case. I do believe that the investigations are ongoing as they were before, and that my expectation is that they will be investigated and prosecuted to the hilt.

Senator SPECTER. Did the FBI chief in San Diego complain to Headquarters or you that he thought her continued presence there was crucial—

Director MUELLER. No.

Senator SPECTER.—To ongoing investigations?

Director MUELLER. No.

Senator SPECTER. Had you heard that the FBI chief in San Diego thought that?

Director MUELLER. I heard from that article, yes, and we followed up. I did not. John Pistol, my Deputy, followed up.

Senator SPECTER. And in what way did you follow-up, and what did it disclose?

Director MUELLER. Well, my understanding is that the—our chief out there believes he was misquoted, but that our investigations were continuing without any diminishment.

Senator SPECTER. The FBI has a Public Corruption section at Headquarters.

Director MUELLER. Yes.

Senator SPECTER. And that unit is designed to follow-up on corruption cases. There's a great deal of controversy, as you know, as to whether New Mexican U.S. Attorney Iglesias failed to prosecute vote fraud cases.

Now, I know that that's a judgment which is made by the attorney and is reviewed by main Justice, but I also have good reason to believe that, as a practical matter, where the FBI conducts the investigations they're intimately involved in it, the agents on the scene have a view.

Was U.S. Attorney Iglesias correct in not bringing a criminal prosecution on that vote fraud matter?

Director MUELLER. I cannot answer that question, Senator. I don't know the facts of it. I will tell you that I had—I had not heard any concern from that office about prosecutorial decisions that were made one way or the other.

Senator SPECTER. In the regular course of your business, do you customarily hear a complaint from your FBI field office?

Director MUELLER. I will in serious cases, yes.

Senator SPECTER. There have been reports that the—that the activities of U.S. Attorney John McKay in the State of Washington raised some FBI concern about McKay's initiatives in Seattle in sharing information. Is there any substance to that issue?

Director MUELLER. I do not—I—I have seen that. I do not know to which that refers. Mr. McKay was innovative in pulling together the—a number of different departments to work together on a combined database. It was funded by the Navy.

And the only issues that ever came up as to what extent—no. To what extent certain pieces or components of the database should be put in this joint database, but it was not a—not a huge—huge issue at all. So I'm not certain what they're referring to in that article.

Senator SPECTER. With respect to the complaint made by the Chief Judge of the Foreign Intelligence Surveillance Court on the reliability of information provided to that court, did that situation have the potential to undermine the confidence of the court and to slow down the issuance of FISA warrants important for national security matters?

Director MUELLER. I do believe, if it were not addressed, that that was a potential. When we learned of the concerns of the court, we put—about the numbers of mistakes that were made in the affidavits, we addressed it with enhanced training, we addressed it with the different procedures to assure the legitimacy of different facts that were articulated.

Senator SPECTER. Let me—let me move on to one other issue before my time expires, and that is the—

Director MUELLER. Can I just finish a second on that, to say that we've put in place these procedures, this compliance program? My understanding is, the initial results are that we have successfully driven down the—the incidence of mistakes. Thank you, sir.

Senator SPECTER. With respect to the national security letters and the misuse of the exigent category—exigent is emergency.

Director MUELLER. Yes.

Senator SPECTER. And it happened on a repetitive basis. The Inspector General said that there was no intentional misconduct. But the report shows that it happened repeatedly and that, at a minimum, there was a reckless disregard for the requirements of law on showing a factual basis for an exigent classification, just again, and again, and again.

How does it happen, Director Mueller, that on matters as important as an affidavit on a FISA warrant, and matters as important as a national security letter on a representation of exigent circumstances, that the agents repeatedly failed to accurately state what the facts are?

That is the basic—that is the basic job of an investigator, is to find the facts and to know the facts and to make an accurate representation on the facts before you get a warrant, a FISA warrant, before you issue a national security letter. How can it be that your highly trained agents make so many factual mistakes?

Director MUELLER. Well, let me—I would make a distinction between the FISA warrant and the FISA package. It's generally a half an inch thick. The affidavits are exceptionally long. You can have thousands of facts in there, and mistakes may be made, although we do our level best to assure that there is no mistake in an affidavit.

With regard to the national security letters, how that happened—in other words, how, over a period of time, persons would sign off on the same form, is something that I've asked our Inspections Division to investigate to determine whether or not steps need to be taken with regard to performance and to determine exactly how that happened and what additional steps we should take in order to address that particular situation.

Senator SPECTER. Director Mueller, I'm not impressed by your assertion that there are thousands of facts. That's your job. That's the FBI agent's job. When you came to us with the PATRIOT Act

and wanted expanded powers, we gave them to you to fight terrorism.

And your agents are supposed to be accurate on the facts, and if they're wrong on the facts, they're subjecting someone to an invasion of privacy, to a national security letter, or to a search warrant that ought not be issued.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Feinstein.

Senator FEINSTEIN. Thank you.

Chairman LEAHY. As I understand it, on our side the order, as I presently have it, would be: Senator Feinstein—we're going back and forth, of course—Senator Cardin, Senator Feingold, Senator Whitehouse, and Senator Durbin. And I've been told on your side, Senator Specter, it would be: Senator Sessions, Senator Kyl, and Senator Grassley, in that order.

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

Good morning, Mr. Mueller. I wanted to begin with something that Senator Specter said. He read to you a section of the January 13 San Diego Union Tribune article that contained the quotes from your FBI agents, and specifically "'Lam's continued employment as U.S. Attorney is crucial to the success of multiple ongoing investigations,' the FBI chief said."

Well, we followed up. I had my chief counsel call them to verify what they said. And they said, yes, they said it, but they also said they'd been warned to say no more. Are you aware that they had been warned to say no more?

Director MUELLER. Yes, I am.

Senator FEINSTEIN. And why would that be?

Director MUELLER. Because I did not think it's appropriate for us to comment on personnel decisions that are made by the Department of Justice.

Senator FEINSTEIN. So if we wanted to find out if there was a link between ongoing public corruption trials, we would then have to bring those FBI agents back here and testify in front of us in public?

Director MUELLER. No, I don't think you would have to do that. We would provide you the information that is necessary, but I do not believe that it's appropriate for our Special Agents in Charge to comment to the media on personnel decisions that are made by the Department of Justice. I am not saying that this Committee does not have the responsibility to follow and determine what the facts are.

Senator FEINSTEIN. Well, I profoundly disagree that he was commenting on a personnel matter, per se. He was simply saying that it would affect cases that were ongoing, and I think he's entitled to his opinion. You're the one—this is the second time, now, you've testified that public corruption is the highest priority of the FBI.

Director MUELLER. Yes.

Senator FEINSTEIN. That's going to mean the investigations are done and the public prosecutions are done. Well, six out of the eight U.S. Attorneys dismissed were carrying out public corruption cases, and that's the investigation that's going on. So if we can't

talk informally, we'll have to bring them back here publicly, which is fine with me.

Director MUELLER. Well, as I say, we are happy to provide the information, Senator, on this issue. The only issue for us was discussing it in the media.

Senator FEINSTEIN. Okay.

Let me go to verbal emergency requests for NSLs. My staff has learned that the authority to issue purely verbal requests extends down to the Assistant Special Agent in Charge level, the second-in-command or higher—

Director MUELLER. Yes.

Senator FEINSTEIN.—At each of the FBI's 56 field offices.

Can you explain why you decided to disseminate this authority so widely?

Director MUELLER. We set out a guidance to the field that was relatively specific with the use of this authority and the situations in which the authority is to be used, and the paperwork that is supposed to accompany any such decision.

Because these decisions can—the request for information can be in situations such as kidnapping or imminent terrorist attack, we believe that the ASAC, given this new protocol, should have the capability of making the oral request. We have found in the past that when it is just the SAC, the SAC may be out of a division for a period of time.

And if you put it at the SAC level, we have had occasions where the SAC has had to, when they are out of that division, they've had to go to another division to get that authority.

And so we've narrowed the—I would say rather substantially narrowed the circumstances in which we would exercise this authority, put in more controls, but by doing so believe that we have to eliminate the problem that you have when you have just the SAC as the only person who could authorize making the oral request. I'd be happy to provide the publication or our guidance to the field so you can see the—

Senator FEINSTEIN. I would—I would like to see it because it's my understanding that you have well over 100 FBI officials now having this authority to issue essentially a verbal emergency request without any contemporaneous paperwork at all.

Director MUELLER. Well, the requirement is that there be contemporaneous paperwork. In other words, yes, you make the oral request, but you have to file—follow it up immediately with a paper.

Senator FEINSTEIN. Okay. Good.

Director MUELLER. It's much like—to a certain extent it's much like the emergency authorities that you have with the FISA court, where you get the oral authority, and then within 72 hours you have to follow it up with the paperwork.

Senator FEINSTEIN. Despite the IG's recommendation that the FBI should keep a control file with copies of all NSLs, it's my understanding that you're implementing a policy that will only keep copies in investigative files because you consider that more appropriate.

So my question is, how is this response sufficient in light of the IG's report's claim that its investigations of NSLs was hampered by the lack of an NSL control file?

Director MUELLER. I'm not certain to what they're referring. I recall a discussion we had in the last few weeks with regard to where we would keep the NSLs and the necessity of having not just one control file, but several control files, depending upon the type of investigation. I would have to get back to you on that—

Senator FEINSTEIN. Right.

Director MUELLER [continuing].—As to exactly how we are requiring, or what file we're requiring, the NSL to be kept in.

Senator FEINSTEIN. I would appreciate that. I believe it's recommendation No. 1 that recommends that all signed NSLs be kept in a control file so that in the future they're accessible.

Director MUELLER. Could you excuse—

Senator FEINSTEIN. Because otherwise the future auditors will be forced to hunt down NSLs from dispersed investigative files.

Director MUELLER. Can you excuse me just 1 second? Maybe I can get a quick answer to this.

Senator FEINSTEIN. Oaky.

[Pause]

Director MUELLER. We actually have—as a result of the discussions we had some time ago, we have established a separate file, not necessarily a control file, not an investigative file, but a particular file to hold these NSLs, and we'd be happy to get more details to you.

Senator FEINSTEIN. In how many locations?

Director MUELLER. In terms of—well, each office would have one. Now, I don't know—

Senator FEINSTEIN. But that's the point. The point is, the number-one recommendation of the IG is to keep them in a central file so that they're accessible for auditors to get at quickly.

And let me just say this. This was a very controversial addition to the PATRIOT Act. There were many members that had deep concerns about this. The language was negotiated. We were very specifically trying to put in the checks and balances and then it appears that they all just melted into oblivion with the sloppy administration.

Director MUELLER. I can tell you, Senator, I'm as disappointed as you in the fact that we did not have the auditing and the compliance capability to assure that we were doing that which Congress anticipated that we would do. And as I have said, we are putting in place, both for NSLs and other areas, a compliance system.

I will—if you excuse me just 1 second on that issue about central location.

[Pause]

I guess this may be a miscommunication. We did not understand Glen Fine to be saying that we had to have them in one office back at Headquarters. We had understood that it is important to have the signed copies readily available for auditors, but they could be in each of our field offices under control. But if you have a different understanding of what he is recommending, we will have to go back and sort that out.

Senator FEINSTEIN. If you'd re-look at that, I'd appreciate it.

Director MUELLER. We would. Absolutely.

Senator FEINSTEIN. Thanks, Mr. Chairman. My time is up. And I have the recommendation here if you want it.

Chairman LEAHY. Thank you.

Senator Sessions.

Senator SESSIONS. I agree with Senator Specter that the war against terrorism is deadly serious business, and I believe there's a clear need for the FBI to have the authority to issue national security letters. We've had a big debate about that and discussed it, and I think we came to a consensus on that.

The new procedures for national security letters provided for in the PATRIOT Act were long overdue and, I felt, extremely valuable in terrorism and counterterrorism cases.

And I think as a practical matter, those national security letter capabilities could be one of the most important, if not the most important, part of the entire PATRIOT Act.

As a practical matter, knowing how investigative agents have to work and the realities of their lives, it provides them information that's important. We also need to remember that the Drug Enforcement Administration, the IRS, OSHA, and other regulatory agencies have the power to issue such administrative type subpoenas on relevant standards, and do so every day for far less serious cases than terrorism cases.

So it's just really—it was always amazing to me that you didn't have the power, on a Friday afternoon or a Saturday afternoon or night, to be able to get an inquiry to make to a motel whether or not some terrorist may be spending the night there. I mean, this is the kind of reality that agents have to deal with and I think it was good, what we did.

So let me ask you, do you think that the national security letters, as a practical matter, are some of the most important aspects of the PATRIOT Act?

Director MUELLER. I absolutely do. I think Glen Fine, in his report, points that out. A substantial section of his report addresses that question because the question was addressed to him by Congress: are these important? And he finds that they are.

But they are the building blocks of our investigation. They are the pieces of information that enabled us to tie Hasmi Mitor to the rest of the hijackers. Had we had this vehicle back in 2001, had we identified these individuals, it would have been national security letters that would have given us the contacts, whether it be telephonic or e-mail contacts, that would have allowed us to identify others, perhaps, as part of the plot.

Senator SESSIONS. Mr. Mueller, you're an experienced prosecutor yourself. You held virtually every position in the Department of Justice and tried many, many cases personally.

Would you explain to us what the difference is between a search warrant—where someone goes into your house and takes your personal records, which is based on an affidavit, probable cause, and other kinds of high standards—and the ability to obtain from a third party, a bank or a telephone company, records that are not private, that were not in the possession of the person you're investigating, but in the possession of a third party?

Director MUELLER. Well, as the Senator well knows, the Fourth Amendment protects the right of persons to be safe in their homes from search. Consequently, unless there are unique and exigent circumstances, one needs a search warrant to do a search in a suspect's home. On the other hand—

Senator SESSIONS. And that means going to a Federal judge and getting that warrant, and you can't go in there until you do that.

Director MUELLER. And you need probable cause to do that search.

Senator SESSIONS. Probable cause. On the other hand, whether it be a criminal case or otherwise, records held by third parties that are not covered by the Fourth Amendment that are subject to, if it's in the criminal context, subpoena by the grand jury, or in the national security context, in various areas of records by national security letter.

Now, that national security letter only applies to these records in the hands of third parties.

Director MUELLER. Correct.

Senator SESSIONS. Not to your personal records, not to your records in your personal office, not your automobile, and not your home.

Director MUELLER. That's correct. And also the national security letter addresses not content of e-mails, not content of telephone calls, but the information called meta data, when it comes to e-mails or telephone toll data when it comes to toll information. That is a key distinction because the intrusion, when you're talking about the content, is far more than if you were talking about telephone toll records or e-mail meta data.

Senator SESSIONS. And if you investigate an individual and believe he or she might be connected to a terrorist entity, you would subpoena the telephone toll records. Not the substance of those calls, just the toll records saying what numbers they called, and if 50 numbers turn up going to 50 different known or suspected terrorist individuals, you know you're on to a significant case, probably, at that point. Is that right?

Director MUELLER. That's correct. Practically—

Senator SESSIONS. Now—

Director MUELLER. Practically, though, if you pulled in a—in an address book that had been found in a—a terrorist safe house and there is a number in the United States, you go look up that number and that number has called 10, or 15, or 20 others, you have to not only identify those who were part of a cell, but also exclude those who had been identified in contact with these individuals, exclude them as being terrorists. So it is as important in identifying those who might be part of the cell as it is in identifying those who should be excluded from further scrutiny.

Senator SESSIONS. Well, this is the basis of investigations every day that have been going on in my 15 years as a Federal prosecutor. I mean, that's what you do every day, you gather this kind of evidence, and we need to get these principles straight.

But I've got to tell you, Mr. Director, that I am disappointed, when you've been given this very valuable power, that we've ended up with this kind of embarrassing failure to properly comply with the regulations and rules this Congress has given you.

Now, you say you take responsibility because you didn't create a sufficient compliance system. I think any manager can say that if you don't set up a compliance system, you're going to have violations. But it seems to me some of your people may well have just not complied with clear directives of the Bureau. Will you take any action—

Director MUELLER. Yes.

Senator SESSIONS [continuing].—To discipline people who—who violated your directives?

Director MUELLER. Yes. I have directed that a thorough inspection be done, investigation be done with regard to the issuance of the exigent letters to determine what happened and how that could have happened, and ultimately whether there ought to be actions taken against individuals as a result of what we find.

Senator SESSIONS. With regard to the Lam situation in San Diego, did she try the corruption case involving the Congressman personally?

Director MUELLER. I don't know what role she had personally in that case.

Senator SESSIONS. Well, isn't it true that U.S. Attorneys come and go frequently, that many of them are sent to Washington for months at a time and that investigations continue by the professional assistants and professional FBI agents that remain there?

Director MUELLER. True.

Senator SESSIONS. And isn't it normally experienced assistants who try big cases themselves for the U.S. Attorney? I tried a few myself, but that was unusual. Most of the time the U.S. Attorney had so much other work to do, and especially in big offices, that professional assistants try the cases.

Director MUELLER. That's true.

Senator SESSIONS. And I will just—and is—what would happen—and this is important. Oh, my time is up. You caught me.

Chairman LEAHY. Finish your conclusion.

Senator SESSIONS. My question would be—

Chairman LEAHY. I said at the beginning of this thing, we're going to have to stick to the clock in the first round.

Senator SESSIONS. You did.

Chairman LEAHY. Because we have many who have to go.

Senator Cardin.

Senator CARDIN. Thank you very much, Mr. Chairman.

It's nice to have you here, Mr. Mueller. Let me go back to the point of national security letters. The information that's requested is very sensitive to the person whose material is being released. And I appreciate Senator Sessions' comments that it might be different than the protections under the illegal searches. The information is extremely sensitive.

The audit has pointed out the misuse, and if it were not for the protections put in for oversight by the Congress, I doubt whether we would be here today and we would have the information about the problems within your agency.

So my first question is the number of national security letters that are requested. Why isn't that information released and made public? What is the reason why that needs to be kept classified?

Director MUELLER. Okay. Excuse me just a second.

[Pause]

Director MUELLER. My understanding, as I thought this was the case, we released the number of records we get. There is some total that is made public. But the breakdown is not made public because it might give those who are looking at how we address terrorism or counterintelligence and the like some idea of our investigative activity. So there is one number that is publicized.

Senator CARDIN. The useful is the number of bits of information you're seeking. The problem we have is that, during some of the debate on the reauthorization of the PATRIOT Act, there was an effort made to find out how often it was being used.

And you released information about the request made under Section 215, but did not do that for national security letters. There was a debate within the press as to how often this was being used. I just think that sometimes we downplay how often this is used.

I'm concerned that you may very well be trying to cast a very broad net to get as much information as you can possibly get. That troubles my constituents because they don't want their information taken inappropriately if it's not with cause.

Second, you're not focusing on the investigation when you—it causes you, your investigators, to be a little bit more sloppy if they're not going to take the time to figure out what they really need.

If we have—if you make public more information that is not vital to protecting the investigation, I think it gives us the ability to help you to focus on what you really need, giving you the authority you really need rather than just letting investigators get as much information as they want, compromising the privacy of the people of this country and jeopardizing the focusing on the importance of investigations.

Director MUELLER. Well, I would be happy to look at what, if any, additional information we can disclose, whether it be to Congress or to the public. But I would have to disagree with the characterization that our agents cast a very broad net.

I would say that our agents follow our investigations, whether it be intelligence or otherwise, to the extent that they believe that there's information that is derivable that will assist the investigation and no further.

A predication for each step of our investigations is an important part of what each and every agent, each and every analyst, and person in the Bureau learns as part of being a member of this agency.

Senator CARDIN. Well, let me switch subjects, because I think it's a similar issue, on the number of people that are included on different lists. The Terrorist Identities Mart Data Environment List that has been filed.

Director MUELLER. Yes.

Senator CARDIN. As I understand it now, it has hundreds of thousands of names on it.

Director MUELLER. Yes.

Senator CARDIN. It includes both Americans and foreigners. It's used for different purposes, as I understand it. And I just question whether that list is tightly guarded. I understand every day new

names are added and there's mistakes, common names, et cetera. It's hard to get off the list once you're on the list.

Director MUELLER. Yes, it is guarded and it is vetted. It is continuously vetted. Continuously vetted. But if we have—I mean, what comes in to TIDE, amongst other things, is information from foreign governments as to putative terrorists who we do not want in the United States. And consequently it is a list not just of persons in the United States, but persons from around the world who are tied into terrorism who we do not want in the United States.

Senator CARDIN. I understand that. Also, there are Americans on that list.

Director MUELLER. Americans are on the—yes, I believe Americans are on that list. Certainly Americans are on the list that is in the Terrorist Screening Center, the one that we use. Absolutely.

Senator CARDIN. Again, I come to the point about making sure you're—that you're careful on whose information you're trying to get. If you've got a common name and you get on a list, and you shouldn't be on the list, it's tough to get off the list. It affects your life. This is very sensitive information to the individual.

I just question whether you have the right safeguards in place. I don't have confidence in looking at the manner in which the national security letters were issued, and I still don't—I'd like to know the number of times you're using it because it's hard for me to understand how often this is being used as to whether it's being judicious rather than saying, we might as well get the information and see if we find something.

Director MUELLER. I understand the concern. I share the concern. We share the concerns with regard to the lists. I know the Department of Homeland Security, ourselves, to the extent we are—have the Terrorist Screening Center, have put in place procedures so that complaints can be filed and ruled upon.

We do continuous vetting to try to eliminate those from the list who no longer deserve to be on the list and have taken a number of steps to reduce the incidence where American citizens or those in the United States spend an inordinate time as a result of their name being similar to somebody else's name on a list. On the other hand—on the other hand, it's absolutely essential.

Senator CARDIN. Let me ask you one more question if I might about Senator Specter's point about your independence to the Congress as far as information that you may have that compromises, for example, the integrity of the U.S. Attorney's Office. Do you agree with Senator Specter's point that if information was brought to your attention through the—through one of your regional offices, that action taken could compromise an investigation by the Department of Justice, would you bring that information directly to our Chairman and Ranking Member?

Director MUELLER. I would have to look at the particular instance. There would be other vehicles that perhaps one could use, whether it be the Inspector General or OPR, depending on the circumstances.

I would have an obligation to assure that that investigation is continued without any fear of influence politically. And ultimately we've had this dialog actually with Senator Specter during my con-

firmation as to, what are the obligations of the Director of the FBI when put in that situation

My belief is, there's an obligation to assure the independence of the investigation and you'll go through whatever steps are necessary to have that assurance, and it may well be briefing the Chairman and Ranking of this committee. I don't exclude that as a possibility.

Senator CARDIN. Well, there's been some very serious charges made in regards to the firing of the U.S. Attorneys.

Director MUELLER. Yes.

Senator CARDIN. And the FBI has been mentioned. We mentioned already Southern California. Have you inquired into your regional offices as to whether there has been a problem perceived by our regional offices in regards to the firing of the U.S. Attorneys?

Director MUELLER. I have not.

Chairman LEAHY. And then after—after this answer—go ahead and complete your answer, then after the answer we'll go to Senator Kyl. Go ahead.

Director MUELLER. Okay. I have not heard of any instance where our investigations have been hampered or hindered as a result of what has occurred.

There was one instance where, unrelated whatsoever to the U.S. Attorneys who have been fired, where an individual came forward believing that in a separate office, separate case, there may have been some political influence, and that particular case, we passed it on to the Inspector General to follow-up on.

Chairman LEAHY. Thank you. Thank you, Senator Cardin.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman.

Thank you, Director Mueller, for your testimony. All of us obviously are concerned about the mistakes identified in the Inspector General's report and are anxious to see that the measures that you have put into place, or will put into place to correct it, are going to work.

We will continue to receive reports from the FBI. There will continue to be oversight by this Committee and the Inspector General will continue to do his monitoring of the situation, and hopefully the combination of those things will tell us whether what you've done will work.

I think it's important for Congress not to compound one set of mistakes with another. And what I have in mind relates to potential legislative changes. I've got a two-part question relating to this, then I'd like to conclude with an unrelated matter.

You testified that the mistakes that were made were not related in the case of the relevance standard. You said that the "the relevance standard is unrelated to the problems that were identified, so the statute didn't cause the errors and should not be changed."

I'd like for you to, A) expand on that. What did you mean by that and why is the relevance standard important to be maintained? And second, what is the reason for what is called the gag rule and whether that should remain as part of the statute, and why?

Director MUELLER. Well, first of all, with regard to the relevance standard, prior to the change in the PATRIOT Act in 2001, we would have to show probable cause before we could get those third

party records, show probable cause that these records related to an individual who was an agent of a foreign power—that agent of a foreign power could be a terrorist—which gets the cart before the horse.

It's very difficult to make that showing without the underlying records, and putting in place the standard—the relevance standard, which is what you find in the criminal arena—gave us the ability to obtain these third party records and build, by developing predication, the basis for going forward with more intrusive methods of investigation, whether it be developing sources or obtaining a FISA wire, and the like.

And those building blocks—those third party records become the building blocks of obtaining the information you need to pursue that investigation, and to go back to revert to some other standard would absolutely handcuff us in our ability to, as people have said, connect the dots, identify potential terrorists. And so in our mind it's tremendously important to keep that relevance standard.

In distinguishing between the standard and what happened, that does not mean that we should not have procedures in place to assure that the safeguards that have been placed in the statute by Congress are not being adhered to.

And so the response in my mind should be, look at the FBI, assure we're putting it in place, the safeguards, the auditing, the compliance, to assure that this doesn't happen again, as opposed to changing the relevance standard.

Now, I may have missed your second question.

Senator KYL. The second question basically was the same question regarding the gag rule. Why—and I know that isn't what the technical name is. But whether it's important to retain the confidentiality of the request.

Director MUELLER. It is. It is, because if you do not retain the confidentiality of the request you will have—are going to—an example would be, we obtain information from MI–5 that a—one of the persons that they're looking at for involvement in terrorism has—is corresponding with somebody with an e-mail address in New York City, New York and providing jihadist literature in the course of what they're sending to New York.

We then would want a national security letter to that ISP to obtain identification of who was using that screen name, that e-mail address, so we can identify that person. If that ISP then goes and tells that person, that's the end of that e-mail account, that's the end of our trail, that's the end of our investigation.

Senator KYL. There was a newspaper account of someone who was very unhappy about the fact that he or she had been served with one of these letters and had to give up the information, and the assumption by this individual that it was overly broad.

Is it quite probable that the individual had no idea what you were seeking and, therefore, would have a very difficult time of judging on his or her part whether it was an improper request and was overly broad?

Director MUELLER. I think that's probably true. What we find in most cases, is we work with the ISP or we work with the communications carrier to provide a request that is on target.

Nobody wants to get reams of information that is irrelevant and often a person, a recipient, will come back and say, hey, look, given the way I keep my records it will take me days, if not weeks, to get this. What are you really looking for? And the request is then narrowed to specifically identify what we need and have the carrier respond.

But if we are to conduct intelligence and criminal investigations into terrorists and be successful in stopping terrorist attacks as—knock on wood—we have since September 11th, we need the ability to obtain this information and to identify persons who are associating with each other for purposes of undertaking or supporting terrorist—

Senator KYL. But not have the information made public.

Director MUELLER. And not have the information made public.

Senator KYL. Let me totally switch subjects. One of the U.S. Attorneys who was asked to resign was the very fine U.S. Attorney in Arizona, Paul Charleton, who has had a running battle with the Department of Justice, one of the reasons that both he and the Department identified as the reason why he was asked to leave, over the use of videotaped or recorded confessions by the FBI.

His view was that they should be, the Department of Justice, relying upon the FBI's view, was that they shouldn't be. His view was that juries would be much more likely to view a confession as legitimate if they could hear it on tape or see it on videotape.

I understand there are reasons both for and against this. I wonder if the FBI would be willing to consider whether, at least in some instances, it wouldn't be appropriate to begin to videotape or record confessions for use in jury trials.

Director MUELLER. Well, for a substantial period of time it's been the discretion of the Special Agent in Charge to allow that. You need the approval of the Special Agent in Charge. The concern we had with the way Paul addressed it, is he indicated he would not take cases unless this had been done.

And at the time, there was a dialog—his view was not necessarily shared by all of the U.S. Attorneys, and there was a dialog with the Department of Justice as to where we should go on this particular—in this particular arena. And so there had been a dialog, and a continuing dialog. And within the last year, I would say, we have given additional guidance to our Special Agents in Charge, liberalizing the incidents of where you would agree to it.

We interview thousands upon thousands of people every day of the year and some of them may end up as defendants, some may not. And it's not a question of just recording the interviews, but also who is going to—if they're recorded, who is going to transcribe them, how are they going to be handled, and they are difficult issues. And the issues differ from jurisdiction to jurisdiction, State to State.

Our concern here was that there was a—I would say a dictate that this is the way you do it, while we were in an ongoing dialog with the Department of Justice, as well as other U.S. Attorneys.

Senator KYL. Thank you very much.

Chairman LEAHY. I might say to the Senator from Arizona, in this day and age where so much is done electronically, the idea of having it recorded, I find very, very appealing rather than notes.

I think it sure cuts down on cross examination, whether your notes are accurate, whether you remembered it correctly, and it's going to be what it's going to be.

Senator KYL. Mr. Chairman, my inclination is to agree with that proposition and to agree with the position of the U.S. Attorney from Arizona. There are reasons the FBI Director has said that they have a different point of view in at least some cases.

I would just note that this is one of those policy differences that was given as the reason for Mr. Charleton's removal rather than any issue relating to his performance, which, by all accounts, was very, very good.

Chairman LEAHY. Without taking up other members' time, perhaps you and I could discuss this further. I think you raise a very good point and we should talk about it more.

Senator Feingold, thank you very much for being here.

Senator FEINGOLD. Thank you, Mr. Chairman.

Chairman LEAHY. You're next. Next is Senator Grassley. If he's not here, it will be Senator Hatch, and then it will be Senator Whitehouse, then Senator Durbin.

Go ahead, Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman.

Welcome, Director Mueller. I appreciate your being here, and also for taking the time to meet with me last week to discuss the Inspector General's report.

Mr. Chairman, I have a statement I would like to be placed in the record.

Senator FEINGOLD. Director, would you agree that without this independent Inspector General audit, these misuses of the NSL authorities might well have never been uncovered?

Director MUELLER. It might well not have, although I would hope that we would—my hope would have been we would have woken up earlier. My hope was we would have identified this as a persistent problem and addressed it, certainly not as soon as the IG did.

Senator FEINGOLD. All right. I appreciate that the FBI is now undertaking its own review and audit of its use of national security letters to follow-up on the IG's findings. I think we both agree that this is long overdue. Will you commit to making public the results of those internal reviews?

Director MUELLER. I would agree to briefing this committee on what happened in those reviews. Where it goes from there, I would—we'll have to see. I don't know whether there are privacy concerns or not—

Senator FEINGOLD. All right.

Director MUELLER [continuing].—But I do believe this committee should be briefed in our findings.

Senator FEINGOLD. Okay.

Part of that review should include a real effort to determine why it took so long for information about certain problems to make its way to your office when it was known by people in the field.

It remains troubling to me that there were warning signs that were apparently ignored or not acted upon appropriately. Do you plan to take a close look at this action and make the necessary adjustments in your internal procedures?

Director MUELLER. Yes.

Senator FEINGOLD. Okay.

The IG report questions whether case agents should be able to "access NSL information about parties two or three steps removed from their subjects without determining if these contacts reveal suspicious connections."

The reason that this is permitted under current law—and I think you were just discussing this to some extent with Senator Kyl—is because the standard for issuing an NSL is mere relevance to an investigation, a very broad standard.

Do you think that the FBI should be able to get the records of an individual three steps removed from a terror suspect without some additional suspicion? Wouldn't that have the potential to cover a lot of innocent people?

Director MUELLER. I think you'd have to look at particular circumstances. Without any rationale, obtaining records from individuals a third or fourth tier away, I do not believe we should because there's no predication for doing that wide a search. But I am not certain we do at this juncture.

In other words, my belief is that the agents will identify the person that's supposed to be associated with a terrorist, then go one, perhaps two, outside because there's predication for doing the next two rings, but third or fourth, there would have to be some predication.

Senator FEINGOLD. But the relevance standard does not require you to do that.

Director MUELLER. Oh, I think it does.

Senator FEINGOLD. You think it does?

Director MUELLER. I think there is an outer limit to the relevance standard, yes.

Senator FEINGOLD. Well, let's take an example. Say you have a suspect and you want to get the phone records of everyone he's in contact with.

Director MUELLER. Yes.

Senator FEINGOLD. And some of these contacts are undoubtedly going to be perfectly innocent, like restaurants he orders carry-out from, or his barber, or his car mechanic.

Director MUELLER. Yes.

Senator FEINGOLD. Should you then be able to get the phone records, or even the credit reports, of anyone who has used those same businesses? Wouldn't that potentially sweep in all kinds of innocent Americans?

Director MUELLER. I think it would in that circumstance. I'm not certain that that would—I mean, I guess you could arguably say that meets the relevance standard, but without more I would say that probably is not an area we should be going.

Senator FEINGOLD. Well, that gets right to the heart of the matter because, understandably, you're defending the relevance standard because of its role in trying to get information in these investigations.

But let me suggest to you that there may be something in between a pure relevance standard and previous law that could try to avoid this very broad interpretation of relevance. And given the record here, given what's happened, we all have reason to be con-

cerned about abuse. I think that's been the message of this. So, I hope you'll be open to that.

At last week's House Judiciary Committee hearing, the FBI General Counsel testified that she believes that one of the root problems laid out in the IG report is that many FBI agents grew up in the transparent criminal system where, as she put it, if they mess up during the course of an investigation they're going to be cross examined. They're going to have a Federal District judge yelling at them.

On the national security side, on the other hand, she explained that actions "are typically taken in secret and they don't have the transparency of the criminal justice system." She suggested that the difference requires a more vigorous compliance system, that more controls are needed in the less transparent arena of national security investigations. Do you agree with that?

Director MUELLER. I do.

Senator FEINGOLD. All right.

Last—

Director MUELLER. And if I might—

Senator FEINGOLD. Yes?

Director MUELLER. I think that is one of the lessons we've learned from this, is if you look at, historically, the FBI as we are changing and transforming ourselves, we have to understand that it's not just transforming ourselves to successfully address the mission, be it counterterrorism or counterintelligence, but we also have to transform ourselves in assuring that we protect the civil liberties and privacy rights of the citizens in ways that may be unique and not comparable to what we have done in the past on the criminal side of the house.

Senator FEINGOLD. And I would add that the distinction here between the regular criminal procedure and what we're talking about here relates as well to the language of the statutes. It is not simply a question of how the procedures and the compliance is done. It has to do with the difference of a word such as relevance in one context or another because of the ability of cross examination and scrutiny by a Federal judge.

Last week I asked the Inspector General his view on the level of intrusiveness of the different NSL authorities. He testified that he believes that the telephone and Internet records authority is least intrusive, and that the authorities for a financial record and credit reports are more so.

Do you agree with that distinction?

Director MUELLER. I've given some thought, because I know we discussed it. It really depends on what you mean by credit reports. I tend to think credit reports are more intrusive because there's more information than you'd have on a telephone toll, but my understanding is credit reports are somewhat ubiquitous now. But the argument certainly could be made that there's a different degree of intrusion when it comes to credit reports as opposed to telephone tolls.

Senator FEINGOLD. For example, he testified that obtaining the details of someone's financial transactions is more intrusive than finding out their bank account numbers. Do you agree with that?

Director MUELLER. Yes.

Senator FEINGOLD. And he testified that obtaining the details about the phone numbers and e-mail addresses with whom someone is communicating is more sensitive than finding out what their own phone number and e-mail address is. Do you agree with that?

Director MUELLER. I'm sorry. Could you repeat that again?

Senator FEINGOLD. He testified that obtaining the details about the phone numbers and e-mail addresses with whom someone is communicating is more sensitive than finding out what their own phone number and e-mail address is. Do you agree with that?

Director MUELLER. Quite probably.

Senator FEINGOLD. Okay.

Thank you, Mr. Chairman.

Chairman LEAHY. Senator Hatch.

Senator HATCH. Thank you.

Welcome to the committee, Director Mueller. I personally am proud of the good work that you do, and you've done for a long time. But, quite simply, we're here to find out how this happened, why it happened, and to make sure it doesn't happen again.

However, I have to disagree with some of my colleagues who call for modifications to the law regarding NSLs, national security letters. As the report states, NSLs in their current form are indispensable tools which are critical for proper and necessary investigations.

And even given my disappointment with this situation, I respect Director Mueller for taking immediate and full responsibility for the shortcomings we discussed today.

Now, the FBI employs more than 30,000 employees across 456 domestic cities and 50 international offices, so there is no way you can possibly know every detail, every case, every procedure or what's on the minds of individual agents all the time.

However, as the Director has rightfully acknowledged, the problems highlighted by this report, you've acknowledged them and you've pledged to fix them. Now that's what the Congress and the American public need, and that's what you've offered, and I appreciate it, personally.

Now, I want to ask just a few questions that I think are important. Some in Congress are using the contents of this report as a reason to repeal portions of the PATRIOT Act as they relate to national security letters. However, the report states that prior to the PATRIOT Act—now, this is the report that they're using to criticize. Prior to the PATRIOT Act, NSLs were not viewed as an effective investigative tool, and that the approval process could sometimes take over 1 year.

Now, how do you respond to those who suggest we legislatively amend NSLs? Isn't that a process which would change NSLs from indispensable to ineffective?

Director MUELLER. Yes, it would. It would handcuff us and inhibit us from doing the kind of investigation that's necessary to thwart terrorist attacks.

Senator HATCH. So you don't want to lose these tools?

Director MUELLER. No, I do not.

Senator HATCH. Although it hasn't received much attention, the Inspector General also reviewed the FBI's use of Section 215 of the

PATRIOT Act. Now, I know you've had some questions on this, but I want to go a little bit farther.

Remember, while this section of the PATRIOT Act was being debated, critics decried its usage and predicted doom and gloom, painting a picture of FBI agents ransacking libraries for people's reading habits. Now, the report shows that this did not happen and found no widespread misuse of 215 orders.

In fact, it appears that the FBI was careful and showed proper restraint in their application. In addition, FBI agents commented that these 215 orders were essential to national security investigations, absolutely essential.

Now, Director Mueller, can you comment about this report and the FBI's use of 215 orders?

Director MUELLER. Well, much of the focus has been on the report on national security letters, but the report on 215 came out exactly the same day and indicated that in that particular arena there was no abuse. There was an appropriate use of that authority.

So I would say, yes, we've got to learn from our mistakes on the national security side, but we also ought to get credit for our handling of our 215 authorities at the same time.

Senator HATCH. How important is that 215 authority to you?

Director MUELLER. Very. It's exceptionally important in a variety of circumstances where we cannot use NSLs, where the intrusiveness—intrusiveness is such that it's important that we have the stamp of the FISA court in order to get particular types of records.

Senator HATCH. Okay.

The Inspector General, in his report, did not find that the FBI agents used national security letters or sought information that they knew they were not entitled to obtain through the letters.

In fact, the IG, the Inspector General, said that in many instances the agents were entitled to the information they received. They were entitled to the information, but they got it in the wrong way. You're aware of that?

Director MUELLER. Yes, sir.

Senator HATCH. This does not appear to be a "power grab" where FBI agents formulated a plan to get information that they knew that they shouldn't get.

Can you elaborate on the assertion that the FBI, in most cases, is entitled to this information?

Director MUELLER. In fact, what the Inspector General found is that there was not an effort to circumvent the statutes or the rules, but that as a result of not fully understanding the authorities, or carelessness, or the like, that a vehicle was used to obtain records that should not have been used, and that in most cases, if not all cases, the agents were entitled to the information and the information was relevant to an ongoing terrorism or counterintelligence investigation.

Senator HATCH. Well, the Inspector General said, in his report, that "our examination of the violations we identified did not reveal deliberate or intentional violations of the NSL statutes, the Attorney General's guidelines, or FBI policy." Nothing was deliberate or intentional, for the most part.

"We believe that some of these violations," they go on to say, "demonstrated FBI agents' confusion and unfamiliarity with the constraints of national security letter authorities."

Now, how do you, as the Director of the FBI, intend to address the confusion of FBI personnel in NSL statutes, and what type of training and education will you provide agency personnel to assure familiarity with these important statutes?

Director MUELLER. Well, it would be on a variety of levels. Everybody in the national security side of the house, the national security branch, will be provided training. We'll assure that everybody has received the training. We have simplified and sent out additional guidance that would enable persons to better understand the procedures that one needs to go through.

But in the end, we have to always make certain that not only is the training given, but the training is assimilated and the individuals on the national security side of the house are adhering to the processes and procedures that have been set up, and we are—we have been for some time, and will continue to develop that process.

Senator HATCH. To be clear, Director Mueller, do national security letters allow for the FBI to obtain the content of communications? In other words, did the abuses listed in the report involve FBI personnel reading e-mails or listening to private phone calls?

Director MUELLER. No, sir.

Senator HATCH. I think that's important because a lot of people thought that it went beyond that. Well, I've only got 15 seconds left. I have one more question, but I'll submit that in writing.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Mr. Chairman.

Welcome, Director. Thank you for your visit the other day, by the way.

You've had a very long and distinguished history in and around the Department of Justice. Just as a matter of personal reference, can you ever recall a circumstance in which an employee of the Department of Justice has exercised their Fifth Amendment rights with respect to their official conduct as an employee of the Department of Justice and remained an employee of the Department of Justice?

Director MUELLER. I wouldn't have—I—I cannot recall. That is because I am not certain—I am not familiar with the circumstances under which this may have come up in the past. I know what you're referring to, quite obviously, and I just cannot answer that.

Senator WHITEHOUSE. I've never—I've never imagined that would happen. I've never heard of it happening before. I was just testing your recollection. You can't think of it ever happening before either at this point?

Director MUELLER. I cannot. But I must say I have not focused on thinking back to circumstances where it may have happened in the past.

Senator WHITEHOUSE. Yes.

Let me go to the NSL issue which we talked about earlier. Seeing it as a systems failure, which I think, clearly, it is, in terms

of the scope of what you intend to do as a response to that systems failure, I wanted to suggest a couple of different levels at which this appears to have failed and check with you whether you agree with me. Obviously the NSL process had failures, correct?

Director MUELLER. Yes.

Senator WHITEHOUSE. And those failures weren't caught and reported to us until the IG process came along, so on top of the NSL failure there was a reporting process failure, which should have caught these. As I recall, it caught 26 errors in 44,000 files and the IG found, what, 17 in 44 files. So there was a reporting failure?

Director MUELLER. Yes.

Senator WHITEHOUSE. Above the reporting failure is an oversight failure, of not having made sure that there was a reporting process in place that actually worked.

Director MUELLER. Yes.

Senator WHITEHOUSE. Would you agree that there was that failure as well?

Director MUELLER. I agree.

Senator WHITEHOUSE. And the fourth, you used the phase "meta data" about the NSL, what's gathered. It strikes me that there was sort of a meta failure as well here of the very, what I would consider to be high-level management failure in your relationship as an executive branch official with the legislative branch of government, vis-a-vis the responsibilities that were conferred on you when the NSL power was expanded in the PATRIOT Act.

It's really that high-level failure that concerns me almost more than any other, because that could apply to any other type of responsibility that is given to you by this Congress with conditions attached.

And there's at least a concern that I think is very legitimate at this point, that somewhere in the FBI—the fact that Congress has attached these critical conditions to a tool that allows you to investigate, in a very private way, Americans' personal records, it didn't get done.

And I'd like to hear you say that, as you address the situation, you take it personally seriously that when Congress gives you a particular set of responsibilities, it is somebody's job very high up in your organization to make darn sure that that gets done, not just because it's the right thing to do, not just as a matter of process down inside the organization, but because your relationship with a coordinate branch of government that gave you this power demands that kind of seriousness toward that other body of government.

Director MUELLER. I agree. And my feeling—it was at the meta level and the oversight level. There are various divisions within the Department, a National Security branch, if you would say, Office of General Counsel, our Inspection Division, all of whom are players or participants in assuring appropriate oversight with various roles to play.

But above that is my responsibility to assure that when Congress gives us these authorities, that I bring into play each of these particular functions within the Bureau to make sure there are no—nothing that falls through the cracks. That, I did not do.

That is what we have to put into place, and the lessons learned on this, regardless of whether it's NSLs or some other area in our National security responsibility, or some area beyond that, in the criminal arena, for instance. So I absolutely agree.

Senator WHITEHOUSE. I would emphasize that I think, particularly under the new leadership in this institution, it's an important point because I think there's a fairly strong sense that for a long time the executive branch has basically blown off Congress, knowing that with Majority control they didn't need to respond to us as a fellow institution. That can't last.

That's not what the founding fathers intended when they set up separated powers and checks and balances, and to make sure that you've really engaged at that level is important to me.

Director MUELLER. Thank you, sir.

Senator WHITEHOUSE. The last question I'd have is with respect to administrative subpoenas. Considering that national security letters can be used to acquire not only meta data from communications carriers, but also financial data from banks and other institutions, and credit data from credit reporting facilities, and so forth.

Are there places where the checks and balances that are built into an administrative subpoena process would be useful to add to the internal process for NSL letters?

Director MUELLER. I would give up NSLs for administrative subpoenas because I think administrative subpoenas are beneficial both to the recipient as well as to our investigators.

I say that because in the regime of administrative subpoenas, there is, generally, opportunity for the recipient to contest it in court on a variety of reasons, but there also is the opportunity for the government to enforce it in court. We do not have an enforcement mechanism for national security letters.

If you talk to individuals who were recipients of national security letters at various institutions, it could be educational institutions, it can be communication carriers and the like. They will give a subpoena preference because of the fact that they understand it is a judicial instrument.

My belief is that adopting an administrative subpoena regimen would simplify it for the agents, and also be advantageous to the recipient, advantageous to the government because of the enforcement or the challenge to enforcement that would come with it, and would be a useful substitute for the NSL letters.

I will tell you, if you look at our NSL authority it's no less than four, and maybe as many as six, separate statutes applicable to a variety of circumstances.

In order to obtain that type of compliance understanding, it's very difficult to simplify. A simpler regiment that persons would understand, whether it be from the perspective of the agent or the recipient, I think, would go—would be exceptionally helpful.

Senator WHITEHOUSE. Okay. Thank you, Director,

Mr. Chairman.

Chairman LEAHY. Thank you very much.

Senator Grassley.

Senator GRASSLEY. Mr. Mueller, I'm supposed to give you the courtesy of having questions I'm going to ask you, so I want to give you the background of those questions before. And this is the—in

regard to Special Agent Michael Jerman. This is a transcript that I'm referring to that we have.

My understanding is that all Special Agent Jerman tried to do was to get the FBI to allow its own rules and acknowledge—to follow its own rules and to acknowledge that a small part of a meeting between white supremacists and an Islamic militant was improperly recorded.

At first, the FBI denied the meeting was recorded at all, and after the transcript surfaced the Inspector General investigated and found that someone at the FBI had falsified records in the case. Unfortunately, the Inspector General could not figure out who did it.

These facts are disturbing, but even worse is that the FBI seems more interested in protecting itself than in developing some human intelligence on extremist groups. An FBI spokeswoman even went on television to deny that the groups discussed working together. The FBI also claimed that the subjects did not discuss terrorism.

After a long struggle, this Committee finally obtained this transcript I've referred to of that meeting directly from the FBI. The transcript repeatedly contradicts what the FBI said and supports what Special Agent Michael Jerman said.

The full transcript has never been made public. It is not classified, but it is frightening evidence of white supremacists and Islamic militants talking about working together. What they have in common, is they're violently anti-Semitic.

For example, in one portion of the transcript the Islamic militant says that "the enemy of my enemy is my friend." The white supremacist agrees. Then the Islamic militant says that anyone "willing to shoot a Jew" is a friend. That does not sound like an innocent meeting between businessmen, and it does sound like two extremists who support terrorism finding common ground with each other.

In other parts of the transcript they talk about their shared admiration for Hitler, arms shipments from Iran, their desire for a civil war in the United States, and their approval of suicide bombings, and, last, assassinating pro-Israeli journalists in the United States. This is all in their very first meeting with each other.

Any sign of cooperation like that between foreign and domestic terrorist groups is exactly the type of intelligence that needs to be identified and distributed to other governmental agencies. That way the whole government can be on the lookout for these groups building operational ties. If the FBI can't recognize the importance of information like this, I don't see how it can serve as effective domestic intelligence agencies.

So my first question is, it's been more than a year since the Inspector General found that Special Agent Michael Jerman suffered whistle-blower retaliation from the FBI supervisor George Martinez.

Has the FBI imposed any discipline on Martinez for retaliating against a whistle-blower? If so, what was the penalty? If not, what has taken so long, and when will this matter be resolved?

Director MUELLER. The answer to the first is yes, but we will be happy to brief you on the circumstances of that within the next several days.

Senator GRASSLEY. Okay.

And then, Director Mueller, have you reviewed this transcript and has the FBI let other intelligence agencies know about it?

Director MUELLER. I have not personally reviewed the transcript. I would have to get back to you on whether or not we have let other agencies know about what's in that transcript.

Senator GRASSLEY. Okay.

Now, it's my understanding that there's no FBI case on either of the subjects in this transcript. Is that true?

Director MUELLER. I'd have to get back to you on that.

Senator GRASSLEY. Okay.

Can you explain why the FBI didn't jump at the chance to infiltrate these organizations instead of wasting the time retaliating against Special Agent Jerman?

Director MUELLER. Well, my understanding is that the Inspector General's investigation found no missed opportunity in that set of circumstances, but I'll have to go back and look at that and get back to you, Senator.

Senator GRASSLEY. Okay.

I have some information, Mr. Chairman, that I want put in the record that I have here.

[The information appears as a submission for the record]

Chairman LEAHY. Without objection.

Senator GRASSLEY. Okay.

And then, last week I wrote to you to ask for copies of unclassified e-mails relating to so-called exigent letters that the FBI used to obtain phone records without issuing a subpoena or following the statutory process for the national security letters.

Those exigent letters contained false statements, and we need to figure out whether the FBI's supervisors signing them knew that they were false. I understand that some of those e-mails will establish that Bassam Youssef reported problems with the exigent letters to the FBI's General Counsel's Office before the Inspector General's Office learned of them. Your staff has indicated that you will provide the e-mails, but we haven't received them.

Why weren't we able to get those e-mails before this hearing, and when will we be receiving them?

Director MUELLER. I'd have to get back to you on the timing of when you'll receive them. I think the e-mails are probably fairly substantial, and before we provide it—those e-mails, we want to make certain that we have the full universe of e-mails that are responsive to the request.

Senator GRASSLEY. Okay.

Youssef said that his supervisors in the operational units at the FBI dismissed his concerns about the national security letters when he took over the Communications Analysis Unit. Why can't the FBI take internal criticism seriously and focus on fixing the problems?

Director MUELLER. Well, we do take internal criticism seriously. As to the assertions there, that is being investigated by Inspections now, who's looking at the full set of circumstances relating to the issuance of the exigency letters.

Senator GRASSLEY. Last week I asked the Inspector General if there needed to be an independent look at the exigent letters

issued to find out who knew what about the misrepresentations, and when they knew it. He said he had not conducted that sort of review, but that you had ordered a special inspection.

Why should we believe that the FBI is capable of investigating itself here, and wouldn't it be better if you asked someone truly independent to get to the bottom of this?

Director MUELLER. Well, in this—in this particular case I think this will be an effective tool, for a couple of reasons. First of all, the—we'll be doing this in conjunction with the National Security Division of the Department of Justice. They will be looking at it. But most particularly, we'll be coordinating with the Inspector General, who is still doing the 2006 review.

We'll be coordinating with the Inspector General and making certain that what we're doing in the course of our investigations does not overlap with what he is doing, and so the Inspector General will have insight into what we're doing, and ultimately this Committee will be briefed on the extent of our information, our investigation, and to the extent that there is—there are issues relating to that, I would hope that I would be able to answer them.

Senator GRASSLEY. I'm done. But let me say one little sentence to the Director. I'm glad that you said you will give answers to us. I won't refer to a meeting that we recently had because you asked us not to, but it was very helpful. I think that you can be more open than you are and eliminate a lot of anxiety I have about whether or not you're being forthright with us.

Director MUELLER. Thank you, sir.

Chairman LEAHY. Thank you, Senator Grassley. Sometimes the promise imposed by the Department of Justice in getting answers back, but there's been several things, and your staff's been keeping notes. We've been saying today, can we get answers back quickly? I hope everybody understands that we're in somewhat of an extraordinary time.

We want those back, and that includes the answers to the questions Senator Grassley, Senator Specter, and I have asked. I'm going to have to leave in a moment. I'm going to yield, for his time, to Senator Durbin first, then Senator Specter will take over. Senator Schumer will take over.

When Inspector Glen Fine released his report on the FBI's use and abuse of national security letters, the committee's distinguished Ranking Member, Senator Specter, said he was very concerned that the FBI has so badly misused national security letters, and I share that concern.

I also saw, just so people won't think this is a partisan thing, in the House Judiciary Committee, Republican Representative James Sensenbrenner called the FBI abuse of the PATRIOT Act authority a "gross overreach".

He also said that he hoped that this would be a lesson to the FBI that they can't get away with this and expect to maintain public support for the tools that they need to combat terrorism. I agree with Congressman Sensenbrenner.

So I hope that after the cameras and the hearing lights are turned off, the bipartisan commitment to conduct meaningful oversight of the broad authorities granted under the PATRIOT Act to

snoop on law-abiding Americans doesn't fade away with the passage of time.

Let's get this thing right. That means honesty on the part of the Department of Justice, it means commitment here. But let's not just have this widespread snooping where you end up with nearly a half a million people, for example, that some way or another are connected on "no fly" lists, and the rest. Then we're doing what we shouldn't be doing.

Director MUELLER. Can I respond just briefly to that, Mr. Chairman, only to say that I would disagree in terms of overreaching. I believe the Inspector General found in almost all cases that the documents that we sought from third parties we could have obtained if we had used the right vehicle. That would be the only comment that I would make, and thank you for allowing me to make that comment.

Chairman LEAHY. Thank you.

Senator Durbin.

Senator DURBIN. Director Mueller, thank you for being here. You occupy a unique place in American history, having been the head of the FBI since 9/11. I believe you came within a few days of that awful tragedy and you've had this responsibility to try to keep our Nation safe in this post.

I'd like to ask you two very general questions to start with which I think reflect why we're here today. Should our Nation accept the fact that violating the privacy of innocent Americans is simply the unavoidable collateral damage of the war on terror?

Director MUELLER. No, and I don't believe—I would disagree with the predicate of that question. We firmly believe that we have to protect the American public, while at the same time protecting civil liberties and privacy concerns. And day in and day out, we try to meet that balance.

Senator DURBIN. Which was my second question, which I believe you've responded to, but I'll state it anyway. Can we keep America safe from our enemies, foreign and domestic, and still preserve our constitutional rights? I take it from your response that it would be in the affirmative?

Director MUELLER. Yes. But I would add that the retaining the standard and the national security letter, the vehicle, is important to our ability to do that.

Senator DURBIN. And I voted for the PATRIOT Act and the reauthorization because I believe you need the tools in this war on terror. But as you've said repeatedly during this hearing, and I've heard you say personally and privately, lessons have been learned in the last few weeks with this Inspector General's report.

Comments that have been made by the General Counsel, Valerie Caprone, when she testified at the House Judiciary Committee, and said "the problem is not with the law." She said, "there is no doubt that the problem with the NSLs was the colossal failure" her words, "on our part to have adequate internal controls and compliance programs in place."

I think a fair analysis of her comment is that she thinks this is a management problem. Our conversation—our private conversation—suggested that there simply should have been closer auditing of what was being done with exigent letters and NSLs.

I disagree with that and I think other members of the panel may as well. I believe there are some fundamental weaknesses and deficiencies in the law that we have given such a broad power to the Department and to the FBI, that it is really open to abuse, and as a consequence, abuses occurred and have not been documented.

I look back on the SAFE Act, which was proposed by a bipartisan group of Senators, conservatives, progressives, Republicans and Democrats, which was summarily rejected by the administration.

One of the things that concerns me is that we are applying a different standard when it comes to the investigation by the FBI, then we are in other investigative circumstances in our government. For example, you and other Justice Department officials have repeatedly compared NSLs to grand jury subpoenas. I think you would concede on the face that they are different, substantially.

Director MUELLER. I'm not certain I would concede that because the standard is the same for grand jury subpoenas as it is for a national security letter.

Senator DURBIN. So let's get into it. In the case of a grand jury subpoena, the government must make a showing of need before a gag order is imposed. Would you support revising the PATRIOT Act to require the government to show a need before a gag order is imposed for a national security letter?

Director MUELLER. No, I probably would not. I'd have to give it some thought. I thought we were talking about the standard. Apart from the standard, if you're talking about the gag—as you call it, the gag rule, I think there has to be a presumption in national security investigations that the fact of the request for the records not be disclosed, but I would be in favor, for instance, of the administrative subpoena mechanism whereby somebody could go to court and challenge the gag letter. In fact, the PATRIOT Act has given them the opportunity. The latest iteration of the PATRIOT Act gives a person the opportunity to go and challenge the gag order.

Senator DURBIN. But you just touched on another fundamental difference between the grand jury subpoena and the NSL, going to court. Under the NSL, no one goes to court. Your agent, or someone within your Department, makes a determination as to whether someone's privacy is going to be invaded or violated. There is no third party judge involved in this case. In fact, a gag order stops those who are subject to this NSL from even protesting the fact that this information has been sought.

Director MUELLER. Well, my understanding is that given the—in the latest iteration of the PATRIOT Act, the person who is the subject of the gag order can go to court and challenge that. And also, in the case of a grand jury subpoena, very rarely does the agent go to court. The agent goes to an Assistant U.S. Attorney. It is not the judge that issues the grand jury subpoena.

The grand jury subpoena is issued pretty much as a matter of course on the relevance standard with regard to our criminal investigations, so I liken it, the NSL, to the grand jury subpoena because they apply the same standard in comparable investigations. I would also add, in the administrative subpoena context we have the administrative subpoena capability for issuing administrative subpoenas in health care cases, in child pornography cases, in nar-

cotics cases, in cases where the threat is much less to the American public than you would have with the threat of a terrorist attack.

Senator DURBIN. Let me go to one other issue, if I might.

Director MUELLER. Sure.

Senator DURBIN. Under the Torture Convention which the United States has ratified, it is illegal to transfer someone to a country where they're likely to be tortured. Nonetheless, the administration has reportedly rendered detainees to countries that systematically engage in torture, including Egypt, Saudi Arabia, and even Syria. Many of these detainees say they were tortured in these countries.

One FBI agent stationed in Guantanamo was so concerned about rendition to countries like Syria, that he wrote a memo which has been made public under the Freedom of Information Act. The FBI agent wrote that sending detainees to a country that uses torture to be interrogated is "a per se violation of U.S. torture statute. This technique cannot be utilized without violating U.S. Federal law."

In a recent MSNBC report, Colonel Britt Mallow, the former Commander of the Defense Department's Criminal Investigation Task Force, and Mark Fallon, the Task Force's chief investigator, reported that the FBI suggested sending a Guantanamo detainee "to another country such as Egypt or Jordan where he can be interrogated with techniques the FBI could not legally use."

Director Mueller, what is your view on rendition? Do you agree with the memo that your agent wrote saying that sending someone to a country where they might be tortured is illegal? And is it true that the FBI recommended sending a Guantanamo detainee to a country like Jordan or Egypt so they could be subjected to these interrogation techniques which would otherwise be illegal?

Director MUELLER. I can respond to the last piece of that question. I'm not familiar with the recommendation of an FBI agent. I would have to look at that. I will tell you that the Inspector General is looking at our role with regard to Guantanamo, what indications of abuse came to our attention, what we did with them. This discussion that you just had or the facts you've just given me will undoubtedly be part of the IG review, but I am not familiar with the third prong of your question.

Senator DURBIN. If I could ask one last question. Recently it was reported that when Secretary Gates took up the head of the Department of Defense, he recommended the closing of Guantanamo and that there was resistance and objection to that from the Attorney General. Were you part of that discussion? If so, what was your position on the closing of Guantanamo

Director MUELLER. No, sir, I was not.

Senator DURBIN. Thank you.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. You look good in that chair. Maybe one day it'll happen.

And thank you, Mr. Director. I'd like to sort of go into some more detail in the direction that Senator Specter took. As you know, we've been looking in, and this Committee has been looking, into the administration's unceremonious dismissals of eight U.S. Attor-

neys. I know you were once a U.S. Attorney in San Francisco, so that must—you know, may bother you.

It's been widely reported that both the White House and the Justice Department have said that some of the fired U.S. Attorneys didn't pursue voter fraud prosecutions aggressively enough for this administration's taste.

And President Bush, by his own admission, passed along to Attorney General Gonzales complaints about certain prosecutors in New Mexico and other States who were perceived as being lax in fighting voter fraud. So I just want to examine that perception with you for a minute.

First, let me ask you, since 2001 has there been any FBI investigation related to election fraud which you believe should have resulted in an indictment, but did not?

Director MUELLER. Not to my knowledge.

Senator SCHUMER. Okay.

Director MUELLER. And none has come to my level.

Senator SCHUMER. Right.

Have you ever heard from your agents about any election fraud case where there were no indictments when they thought that there should have been?

Director MUELLER. I have not.

Senator SCHUMER. Has any Special Agent in Charge ever brought such a case to your attention?

Director MUELLER. No, sir.

Senator SCHUMER. And have you ever asked FBI personnel about election fraud cases in which indictments should have resulted, but did not?

Director MUELLER. No.

Senator SCHUMER. Okay.

Have you ever been asked by officials at the DOJ or elsewhere in the administration about the FBI's view on how a specific election fraud case was handled by prosecutors?

Director MUELLER. No.

Senator SCHUMER. Were you consulted in any way about the performance of any of the fired U.S. Attorneys with respect to election fraud cases?

Director MUELLER. No.

Senator SCHUMER. Did you ever talk to Kyle Sampson, the Attorney General's former chief of staff, about the performance of the fired U.S. Attorneys?

Director MUELLER. I can't recall having any specific—I certainly was not consulted and I cannot recall any specific conversation I may have had with him. To the extent that I had any conversation, it probably was with regard to San Francisco because I was a U.S. Attorney there, and I believe that that U.S. Attorney was one of those who was asked to leave.

Senator SCHUMER. Mr. Ryan.

Director MUELLER. And so I'm not discounting the possibility of some conversation, but I have no recollection.

Senator SCHUMER. You don't recall any conversation.

Director MUELLER. No. No.

Senator SCHUMER. And how about any conversation about these fired U.S. Attorneys and their performance with the Attorney General?

Director MUELLER. No.

Senator SCHUMER. Okay.

Now I'd like to go into a couple of specific examples, because these came up. First, is John McKay. He's the former U.S. Attorney in the Western District of Washington. He faced complaints about his decision not to prosecute allegations of election fraud in the very close 2004 gubernatorial election.

Mr. McKay said that here was "no evidence" of election fraud and that he would have resigned if he had been told to pursue a case. Now, isn't it true that the FBI agreed with Mr. McKay's decision not to prosecute that case?

Director MUELLER. I'm not familiar with our position on it.

Senator SCHUMER. Could you get back to us in writing on that?

Director MUELLER. Please let me think about that. I'm not certain. I would have to consider whether that kind of information into our investigative—

Senator SCHUMER. Okay. The reason I ask is, it was Mr. McKay who said that the—I just want to get corroboration here. This is not—

Director MUELLER. Let me get back to you on that if I could.

Senator SCHUMER. Okay.

Director MUELLER. I don't want to open—I would want to consider providing that kind of information in a case that did not go forward. That would be unusual.

Senator SCHUMER. Here's what—just so you know, here's what Mr. McKay said. He said the FBI "concurred with the State trial court judge that there was no evidence of election voter fraud in that election." So would you just check with me and check on that—

Director MUELLER. Yes.

Senator SCHUMER.—and see if you can get back? Okay.

Maybe this. Just in case, although you're not familiar with it—you don't recall having any discussions about this yourself, I imagine, right?

Director MUELLER. What do you mean by—

Senator SCHUMER. The McKay situation.

Director MUELLER. The McKay? No. I did not have any discussions with him.

Senator SCHUMER. Okay. Because, again, he said that his prosecutors worked with FBI agents to review the fraud allegations and to look at every piece of evidence in the State court—in the State court case challenging the election.

He said he then made the decision not to pursue that case after full consultation with the Department of Justice, and after all that, he didn't find enough evidence. So I would again ask you, this is serious. We want to see if Mr. McKay's recollection—I have no reason to doubt. It is corroborated.

So I'd really like you to provide for us, within a week, copies of any documents in the custody, control, or possession of the FBI regarding allegations of election fraud in Washington and the FBI's recommendations in that matter. I'm going to send you a letter to

that effect. I'm going to send you a letter to that effect. But I don't see any good reason why you shouldn't allow that, do you?

Director MUELLER. I would have to think about that.

Yes, I can see that—we would have to think about that.

Senator SCHUMER. Okay.

Director MUELLER. I would have to consult with the Department of Justice.

Senator SCHUMER. Okay.

Director MUELLER. Quite obviously, where we decide not to go forward, disclosing investigative materials may set a precedent that will affect or infect other things down the road.

Senator SCHUMER. Okay.

Director MUELLER. So I'd have to give some thought to that.

Senator SCHUMER. Okay.

Off the top of my head, I wouldn't mind, if you're worried about somebody's name being out there, you know, someone—not an FBI agent, but some possible person who might have been alleged to commit voter fraud, if you want to redact names, in this case I think that would be all right.

I just want to just get clear that the FBI backed up Mr. McKay, because again, he's totally befuddled by this idea that he didn't—you know, that he was—why he was fired, and this is a possible reason. I just want to make sure that there was no basis for it.

Director MUELLER. Well, let me, if I could, look at the request and see what we could do to accommodate it.

Senator SCHUMER. I'm going to go through questions with you on a similar case. This is David Iglesias, which I believe Senator Specter talked about. He was the former U.S. Attorney from New Mexico. He was criticized for his handling of allegations about flawed voter registration cards. That was in the 2004 election.

He says that he set up a task force, investigated these allegations fully, but he didn't find enough evidence to prosecute anyone. Again, isn't it true that the FBI agreed with Mr. Iglesias's decision not to proceed in that case?

Director MUELLER. Again, I do not know. I will respond to the request for the records, as appropriate.

Senator SCHUMER. Okay. Okay.

In other words, since all this has been in the papers you haven't asked anybody about it?

Director MUELLER. I have not been informed. No, I have not asked anybody about it and I have not been informed one way or the other as to the accuracy of the statements either by Mr. Iglesias or Mr. McKay.

Senator SCHUMER. Okay. Let me just, again, state what he said. Mr. Iglesias said that the Justice Department—he said that he didn't enough evidence to pursue the charges, and his quote is that "the Justice Department and the FBI did not disagree with his decision in the end not to prosecute." So we'd want all information about those.

Now, this is about general complaints about voter and election fraud. Has the Attorney General ever conveyed to you complaints about how the FBI was handling any specific election fraud matter or about the FBI's conclusion in an election fraud case?

Director MUELLER. No.

Senator SCHUMER. Okay.

And how about the White House or any other public official in the same area?

Director MUELLER. No.

Senator SCHUMER. Okay.

Based on your testimony—well, I guess we're going to have to wait for written information about the cases that I've asked.

And with that, let me just go here. Okay. Let me ask you this. This, again, relates to the same topic. You served as a U.S. Attorney, first in Massachusetts and then in the Northern District of California. Is that right?

Director MUELLER. Yes, sir.

Senator SCHUMER. And when you were a U.S. Attorney were you ever contacted by Department of Justice officials? Just give us the years for that, just so the record—approximately.

Director MUELLER. I was Acting U.S. Attorney in Boston probably from 1986 to '88. I was U.S. Attorney in San Francisco from approximately 1999 to 2001.

Senator SCHUMER. Thanks. Okay.

Director MUELLER. I was in both those offices for longer, but those are my times.

Senator SCHUMER. Understood.

When you were a U.S. Attorney were you ever contacted by Department of Justice officials, White House officials, or other public officials about a specific case?

Director MUELLER. Surely.

Senator SCHUMER. You were? Okay.

Let me ask you, did any administration or public official pressure you and tell you not to prosecute a case or try to get you to prosecute a case that you didn't think should be pursued?

Director MUELLER. I mean, that's, unfortunately, a fairly broad question.

Senator SCHUMER. It is.

Director MUELLER. But there are cases that have international ramifications, for instance.

Senator SCHUMER. Right.

Director MUELLER. If I indict the head of a country someplace—

Senator SCHUMER. Right.

Director MUELLER.—the State Department gets—without being alerted, or even if alerted, gets unhappy. So there are a number of considerations in the cases, and the question is so broad. Yes, there are—

Senator SCHUMER. But I'm talking about specific pressure, you ought not do this, for external reasons.

Director MUELLER. Yes. But I think what you're getting at is political or partisan political reasons.

Senator SCHUMER. Correct.

Director MUELLER. And I cannot recall that happening, if that's the thrust of the question.

Senator SCHUMER. Good. Well, that was my next question. Okay. Good. Okay.

Well, here's what I want to ask you. So let's say, as a U.S. Attorney, you did receive that kind of pressure. You resisted it, which

I imagine you would, knowing you and your reputation. Then you were, 2 months later, fired.

You were told, we're not giving you a reason. Then it turns out that they said you were fired for incompetence, but you hadn't really heard about any specific incompetences as you were U.S. Attorney. How would you feel about that?

Director MUELLER. I'd really have to resist speculating on that set of facts.

Senator SCHUMER. I figured you would. Okay.

I thank you, Mr. Chairman. My time has expired.

Senator WHITEHOUSE. At that point, Director, this concludes the hearing. I want to let you know how much I appreciate your testimony and your long and extremely distinguished service to the country, and your candor to the Committee today. We will leave the record of the Committee open for a week so that you may add to it, if that's enough time.

Director MUELLER. Thank you, sir.

May I just check one thing, if I might, before we close?

Senator WHITEHOUSE. Yes.

[Pause]

Director MUELLER. Okay. Well, that's great. Okay.

Senator WHITEHOUSE. The hearing is adjourned.

[Whereupon, at 11:54 p.m. the hearing was adjourned.]

[Questions and answers and submissions for the record follow.]

U.S. Department of Justice

Office of Legislative Affairs

QUESTIONS AND ANSWERS

Washington, D.C. 20530

January 25, 2008

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Please find enclosed responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on March 27, 2007. The subject of the hearing was "Oversight of the Federal Bureau of Investigation."

The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of this letter. Please do not hesitate to contact this office if we may be of further assistance with this, or any other matter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosures

cc: The Honorable Arlen Specter
Ranking Minority Member

**Responses of the Federal Bureau of Investigation
Based Upon the March 27, 2007 Hearing Before the
Senate Committee on the Judiciary
Regarding FBI Oversight**

Questions Posed by Senator Leahy

NATIONAL SECURITY LETTERS

1. Despite the recent report by the Department of Justice Inspector General finding illegal and improper use of National Security Letters and so-called "exigent letters," I understand that the FBI may still be using exigent letters. Is the FBI still using exigent letters and if so, why have you not stopped this practice?

Response:

Effective March 1, 2007, the FBI prohibited the use of "exigent letters" as they are described in the report by the Department of Justice (DOJ) Office of the Inspector General (OIG) (that is, a letter that simply asserted that exigent circumstances existed and advised that a grand jury subpoena or national security letter (NSL) had been requested when, in fact, it had not). That practice has been stopped. The OIG objection to the "exigent letters" rested on several facts: (1) there was not always a true emergency and, even when there was, it was not documented; (2) the letters appeared to be coercive; (3) the letters advised that future legal process of a particular type (grand jury subpoena) had already been requested when, in fact, no legal process had yet been requested and the anticipated future legal process was different from that described in the letter; and (4) in many cases, the future legal process was not delivered at all or was delivered months later.

Emergency disclosures by communications service providers to the government pursuant to 18 U.S.C. § 2702(c)(4) are entirely lawful and will continue under appropriate circumstances. Section 2702(c)(4), which has been a part of the Electronic Communications Privacy Act since 2001, provides that an electronic communications service provider may voluntarily disclose to a governmental entity a record or other information pertaining to a subscriber or customer (other than the contents of communications) if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay. On March 1, 2007, the FBI reaffirmed its intention to continue to use this valuable tool, setting out clear procedures for invoking this provision. Pursuant to this process, the FBI can present a provider

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.061

with information indicating the existence of an emergency and asking the provider to produce covered information. Pursuant to these procedures, the FBI Special Agent (SA) seeking the records must make clear to the provider that any production of documents is entirely voluntary, no other legal process may be promised, and, by policy, the emergency justifying the request must be documented.

2. The Attorney General's guidelines require that the FBI use the least intrusive investigative tools to obtain the information that it needs. During the recent hearing that the Committee held on NSLs, Inspector General Glenn Fine testified that the least intrusive NSL are the ones seeking telephone records and that NSLs for financial records and for credit reports are more intrusive of Americans' privacy. During the hearing, you testified that you believed that NSLs seeking credit reports could be intrusive, but less so than those seeking telephone toll records. Does the FBI have a policy in place requiring that agents first use the least intrusive types of NSLs - such as NSLs seeking telephone toll records - when conducting investigations? If not, will you adopt such a policy to better safeguard Americans' privacy?

Response:

The requirement to use the "least intrusive means" originates in Executive Order 12333 and is reiterated in Attorney General (AG) Guidelines. This mandate applies to all intelligence activities conducted by the FBI, and generally requires consideration of the relative intrusiveness of various investigative techniques. For example, obtaining toll billing records from a communications service provider is clearly less intrusive than searching a subject's home for the same information. The FBI's Office of the General Counsel (OGC) is drafting advice to the field to assist SAs in applying the "least intrusive means" concept during national security investigations.

3. I am also concerned about the kind of information that the FBI is seeking in its National Security Letters.

a. Is it true that most of the FBI's NSLs seeking telephone or Internet records under the Electronic Communications Privacy Act ("ECPA") seek only subscriber identifying information? What percentage of these NSLs seek other transactional information, such as toll records or billing records?

Response:

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

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.062

b. With regard to NSLs that seek bank or other financial records under the Right to Financial Privacy Act, the Fair Credit Reporting Act and the National Security Act, what percentage of these NSLs seek detailed financial transaction information, such as bank account records and/or full credit reports?

Response:

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

4. During the hearing, you testified that the information that the FBI improperly obtained through unlawful NSLs has been placed into the FBI's database. What steps have you taken to track all of this improperly obtained information, and have you removed it from all of the FBI's files and databases?

Response:

The FBI's Inspection Division has been directed to investigate the use of NSLs as an investigative tool in all 56 FBI field offices and at FBI Headquarters (FBIHQ) to address the concerns raised in the OIG report. Both the Inspection Division and the OIG are also taking an additional, and closer, look at the use of "exigent letters" by the FBIHQ unit identified in the OIG report. If any of those reviews reveal that the FBI used "exigent letters" to obtain information that was not relevant to an authorized national security investigation, that information will be removed from the FBI's databases and destroyed.

5. Has any of the information improperly obtained through unlawful NSLs been used in any criminal cases or investigations and, if so, have you notified appropriate authorities at the Justice Department in order to make sure none of this information has been improperly used in our justice system?

Response:

The information obtainable through NSLs, the overwhelming majority of which is subscriber information or toll billing records, would only rarely be used as evidence in a courtroom. Such information is typically a very small part of a very large and complex investigation, most often a small stepping stone through which one terrorism subject is linked to others. The primary benefit of NSLs is not to obtain evidence for criminal prosecutions (which is more the function of other vehicles, such as grand jury subpoenas), but instead to obtain leads to other information; these pieces of information form the building blocks of national security investigations. In popular parlance, NSLs allow us to obtain "dots" that can be connected to lead to the identification and disruption of terrorist networks.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.063

As indicated in response to Question 4, above, if the FBI determines that we have obtained through exigent letters information that was not relevant to an authorized investigation or was not obtained in conjunction with an actual emergency, this information will be removed from FBI databases. In addition, a report to the President's Intelligence Oversight Board (IOB) will be made in appropriate cases.

6. Do you believe that the FBI's failure to follow the law in obtaining NSLs may be exculpatory, or *Giglio* information, that needs to be disclosed if the information is used in court?

Response:

Under the circumstances in which these NSLs and the NSL-derived information have been used, we do not believe the shortcomings identified in the OIG report constitute exculpatory, or *Giglio*, material. We understand, however, that what might be helpful to an individual defendant or might bear on the credibility of a witness in an individual case can be very fact-specific. If the OIG, OPR, or the FBI's Inspection Division determine that an FBI employee violated the law relative to the use of NSLs, that information might constitute impeachment material if that employee were subsequently to testify in a related criminal proceeding. In such a circumstance, the information would be provided to the appropriate Assistant United States Attorney (AUSA) for evaluation. Likewise, if a particular criminal defendant were to move to suppress or dismiss based on an alleged improper use of an NSL, then facts about that particular NSL might be relevant. We would note, however, that there is not typically a suppression remedy for violations that do not rise to a Constitutional level.

7. The Judiciary Committee has received letters and briefings from FBI and Justice Department officials in the past, assuring us that NSLs were being used properly, and that all appropriate safeguards and legal authorities were being followed. For example, in a November 2005 letter to this Committee (attached), the Justice Department asserted emphatically that the FBI was not abusing the process for seeking NSLs, and that all NSL activity was accurately being reported to Congress as required by law. In light of the Inspector General's report, will you review those letters and briefings to see if anyone at the FBI or the Justice Department has misled this Committee about NSLs?

Response:

The FBI has acknowledged shortcomings in its efforts to ensure adequate safeguards were in place to oversee the use of NSL authorities and in tabulating data the for purposes of Congressional reporting. There are ongoing

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.064

investigations by the FBI's Inspection Division, DOJ's OIG, and DOJ's Office of Professional Responsibility (OPR). If any of these investigations indicate that an FBI employee intentionally misled Congress, appropriate steps will be taken and our Congressional oversight committees will be informed.

8. According to the Inspector General's report, one of the major reasons that the FBI failed to report thousands of NSLs to Congress was because of a malfunction in a FBI's computer database. Apparently, this breakdown occurred in 2004, causing the loss of information about more than 8,000 NSL requests. What was the cause of this malfunction, and have you corrected it? Why did you fail to report this problem to Congress?

Response:

What the OIG report described as a "crash" and data loss appears to have been an incident in which the creator of OGC's NSL database was locked out from accessing the database. That lock-out was bypassed by a technician, who imported the data into a new database. The "glitch" was fixed and there appears to have been no loss of data.

Review of the data since release of the OIG report reinforces our belief that no data was lost. We are discussing our review with the OIG in an effort to reconcile our disparate conclusions and are continuing to work to determine the extent of data entry errors that affected prior Congressional reporting.

9. You testified during the hearing that the FBI has revised its internal policy on NSLs and adopted the recommendations contained in the Inspector General's report. But, in 60 percent of the NSLs that the Inspector General reviewed, he found widespread failure on the part of the FBI to comply with its own internal control policies. Given this track record, how can you assure Congress that the new policies that you are implementing will prevent future abuses of NSLs, when the Bureau clearly failed to follow its own policies in the past?

Response:

The IG did not find that 60 percent of the NSLs reviewed had mistakes. The IG reviewed 293 NSLs and found 22 errors (7 percent) that he classified as potential errors that should be considered for reporting to the President's IOB. Of the 22 errors the IG identified as potential errors, 10 were third party errors (i.e., the recipient of the NSL provided the FBI information that was not requested). The remaining 12 out of 293 NSLs examined (or just 3.4 percent of all NSLs examined) are FBI errors. But even that statistic overstates the number of NSLs that "misused" the NSL authority. Of the 12 errors attributable to the FBI, 2 involved full credit reports in counterintelligence investigations, and 1 involved

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.065

information that was arguably content from an electronic communications company. The remainder of the errors did not affect anyone's statutory rights and are best characterized as administrative errors on the FBI's part. Thus, only 3 of the 293 NSLs reviewed (1 percent) contained significant errors.

Nevertheless, the FBI took the IG's findings very seriously. Following the OIG report, the FBI has prepared comprehensive guidance concerning the use of NSLs. Every proposed NSL must be reviewed by the Chief Division Counsel in each FBI field office or by an attorney in OGC's National Security Law Branch (NSLB) at FBIHQ, including review of the relevance of the request to an authorized investigation and the predication for that investigation. In addition, NSLB is developing a training curriculum, which will be mandatory for all employees involved in the NSL process, to address problems created by confusion and lack of familiarity with the provisions and requirements of the various statutes authorizing NSLs. Even before the OIG report was published, the FBI had begun work on a database, based on the successful "FISA Management System," that will permit the electronic transfer of NSL-related data between databases (this transfer is currently being accomplished manually). Finally, the FBI's Inspection Division is investigating in more detail many of the problems identified in the OIG report. This review should identify any areas that require closer scrutiny. Taken together, these measures will both provide a more user-friendly business process for FBI personnel who use NSLs as an investigative tool and enhance management's audit and oversight capabilities. This system will also enhance the accuracy of the NSL reports provided to Congress.

The FBI has also recognized the need to create a compliance program to ensure we have appropriate policies, procedures, audit capabilities, and training for all our activities. The FBI's compliance program will be modeled after similar programs in the public and private sectors. While it is too early to say with certainty what the program will look like, it will most likely incorporate features common to most successful programs, such as a written compliance policy, a central compliance officer and office, a senior-level compliance committee, access to and the ability to draw upon the resources of the organization, and an implementing strategy that adjusts as new threats and programs are identified. Audits of practices, not just procedures, will be an essential component of the program, as will effective "two-way" communication channels. In addition, OGC will continue to meet s regularly with DOJ's National Security Division (NSD) to discuss appropriate policies in the national security arena.

In addition, DOJ's NSD and the FBI's NSLB, along with officials from DOJ's Privacy and Civil Liberties Office, will conduct at least 15 national security reviews of the FBI's field offices in calendar year 2007. Those reviews will

6

These responses are current as of 7/31/07

38189.066

broadly examine the FBI's national security activities, its compliance with applicable laws, policies, and AG Guidelines, and its use of various national security tools, including NSLs. The reviews are not limited to areas in which shortcomings have already been identified; instead, they are intended to enhance compliance across the national security investigative spectrum. At the AG's direction, the NSD will also review all referrals by the FBI to the President's IOB, focusing on whether these referrals indicate that changes in policy, training, or oversight mechanisms are required. The NSD will report to the AG semiannually on such referrals and will inform DOJ's Chief Privacy and Civil Liberties Officer of any referral that raises serious civil liberties or privacy issues.

10. During the hearing, you testified that "[t]he relevant standard established by the PATRIOT Act for the issuance of National Security Letters is unrelated to the problems identified by the Inspector General." Yet, given the broad scope of the abuses uncovered by the Inspector General's report, it appears that there is a need for additional checks and balances on the authority to issue NSLs. Do you believe that an independent check on the NSL process, such as approval of NSLs by a judge, a Justice Department attorney, or an outside review panel, would improve the NSL approval process and prevent future abuses?

Response:

We do not agree that the OIG uncovered "a broad scope" of FBI abuses. On the contrary, the OIG report identified a problem in one FBIHQ unit that used exigent letters. The unreported IOB violations identified by the OIG (at p. X of the report) do not reflect widespread abuse by the FBI; while 22 of the 293 NSLs reviewed by the IG (7.5 percent) were said to indicate some sort of violation, 10 of these 22 NSLs (45 percent) were the result of a third-party error in providing the FBI with material outside of the request. As discussed in response to Question 9, above, of the 12 errors attributable to the FBI, 2 involved obtaining full credit reports in counterintelligence investigations, and 1 involved obtaining information that was arguably content from an electronic communications company. The remainder of the errors did not affect anyone's statutory rights and are best characterized as failures of care on the FBI's part. Thus, only 3 of the 293 NSLs reviewed (1 percent) contained significant errors. We do not minimize those errors, and we recognize that the OIG's follow-up NSL investigation, which is ongoing, may identify additional problems in the FBI's use of NSLs, but we believe that requiring either a court or an AUSA to approve an NSL would be an overreaction to the level of error, and may not have prevented one of these errors. We have taken significant steps to reduce that 1 percent error rate without altering the approval process. For a more complete discussion of the steps the FBI has taken in this regard, please see our response to Question 9, above.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.067

Finally, we note that altering the NSL approval process to require review by a judge, DOJ attorney, or outside panel would largely eviscerate the usefulness of this tool. Such a change would likely result in either a significant slowing of our national security investigations, with possible adverse impact on our national security, or abandoning NSLs in favor of grand jury subpoenas when possible. Grand jury subpoenas are less transparent than NSLs because they include no reporting requirements. Moreover, if we were to lose the efficient use of NSLs in terrorism investigations, we would have the anomalous result that our investigators would have access to more agile tools to investigate narcotics and child pornography (where administrative subpoenas have long been available) than they do to investigate threats to our national security.

LIBRARY RECORDS

11. I appreciate your March 30, 2007, letter responding to my question about how often the FBI has used NSLs to obtain records from libraries and educational institutions. In your letter, you state that the FBI's Office of General Counsel has maintained an informal list of the number of NSLs served on educational institutions or libraries; however, you also state that this list may not be complete or accurate. Given the importance of this issue to Americans' privacy and civil liberties, will the FBI agree to formally track the number of NSLs issued to libraries and educational institutions and periodically report this figure to Congress?

Response:

The FBI will track NSL recipients and will be pleased to address related inquiries by our Congressional oversight committees. It is important to note that the FBI does not serve NSLs on libraries or educational institutions per se, but instead on "electronic communication services" and "financial institutions" as those terms are defined in the statutes authorizing NSLs. Similarly, the FBI would direct a Right to Financial Privacy NSL to an educational institution only if it were providing financial services to its employees or students.

12. During the hearing, you cited the Inspector General's Report on Section 215 of the PATRIOT Act, which found that the FBI rarely used this authority to obtain library records. However, I am concerned that the FBI is using other provisions in the PATRIOT Act to obtain this information, thereby circumventing the safeguards and reporting requirements of Section 215. For example in 2005, the FBI issued NSLs to four Connecticut libraries asking them to surrender "all subscriber information, billing information and access logs of any person" related to a specific library computer during a specific time period, pursuant to Section 505 of the PATRIOT Act. These NSLs also

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.068

prohibited the librarians from disclosing the fact that they had received the NSLs or their contents -- the so-called "gag order" under the PATRIOT Act.

a. Please describe the circumstances surrounding the FBI's decision to issue these National Security Letters.

Response:

We believe the report that NSLs were served on four Connecticut libraries is erroneous. The FBI served one NSL on the Executive Director of Library Connections, Inc., an Internet service provider that furnishes computer services to several libraries. No library was served. Three directors of Library Connections, Inc., have apparently described themselves as individual NSL recipients, but the case agent who served the NSL on one official had no contact with the others.

This one NSL was issued in order to follow up on an alleged local connection to international terrorism. The FBI sought subscriber information, toll billing records, and logs relative to those who had access to the communications services during relevant times. The NSL was very narrowly tailored to seek information for only a 45-minute period.

b. Please identify all of the PATRIOT Act provisions that the FBI has used to obtain library records from libraries and educational institutions?

Response:

We understand the term "library records" to mean records of libraries that reflect loans of books, movies, and similar materials to library patrons. We are not aware of any use of the USA PATRIOT Act to obtain such "library records" from educational institutions or libraries. As indicated in the previous response, we are aware that one NSL was served on a company that provides computer services, including Internet access, to several libraries. This NSL was authorized by 18 U.S.C. § 2709, which was amended by section 505 of the USA PATRIOT Act.

c. Is the FBI circumventing the requirements of Section 215 by relying on other provisions in the PATRIOT Act to obtain this information?

Response:

The premise of this question appears to be that the sole authority for obtaining information from a library or educational institution is section 215 of the USA PATRIOT Act. In fact, libraries and schools are subject to grand jury subpoenas

and NSLs under certain circumstances. If a library provides Internet service that meets the definition of an electronic communication service, as defined in 18 U.S.C. § 2510(15), then the library is an electronic communication service provider to which the provisions of 18 U.S.C. § 2709 apply. Similarly, while special rules govern the acquisition of a student's records from a university, an NSL can be used to obtain toll billing records if the school is functioning as a telephone company relative to the provision of campus telephone services.

ARAR/WATCHLIST

13. I have asked before about Maher Arar, a Canadian citizen who when returning home from a vacation in 2002, was detained by federal agents at JFK Airport in New York City on suspicion of ties to terrorism, and was sent to Syria, where he was held for 10 months. After I pressed the Attorney General about the Arar case at a hearing in January, Senator Specter and I were finally granted a classified briefing. After that briefing, we wrote to request a Justice Department investigation into the matter and have learned that the Department's Office of Professional Responsibility is looking into the Department's legal decisions.

a. Is the FBI taking any steps to evaluate whether your agents and officials acted properly in the Arar matter, particularly with regard to the original decision to send him to Syria, rather than to Canada?

Response:

DOJ's OPR opened an investigation based on a referral from the Department of Homeland Security (DHS) OIG concerning the detention and subsequent removal of Maher Arar, a Canadian citizen, to Syria from JFK Airport in New York City. The FBI's Inspection Division conducted an internal review of the actions of FBI personnel with respect to this matter. The FBI will cooperate fully with the DOJ OPR review and will defer final adjudication regarding the of actions of FBI personnel until the DOJ OPR review is concluded.

b. Given that a past OPR investigation of a politically sensitive matter, specifically the NSA's warrantless wiretapping program, appears to have been blocked, will you commit to cooperate with OPR's investigation of the Arar case?

Response:

The FBI cooperates with DOJ's OPR on an ongoing basis, and commits to continuing to do so as appropriate in this matter.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.070

c. What steps has the FBI taken to ensure that you do not participate in sending other people in the future to places where they will be tortured?

Response:

As a signatory to the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment ("The Convention Against Torture," or "CAT"), it is the obligation of the United States not to "expel, return ('refouler') or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture." (CAT, Article 3(1).) The department with primary responsibility for knowing the human rights record of foreign countries (and, therefore, knowing whether there should be concern about potential violations of the CAT) is the Department of State. The FBI does not have the authority to deport people from the United States, to determine the country to which a deportee will be delivered, or to ascertain whether such a deportation might run afoul of the CAT. Our role in deportations is to share whatever relevant information we might possess to assist the agencies that do have those responsibilities to fulfill them.

14. Despite having been cleared of all terrorism allegations by Canada, Mr. Arar remains on a United States terror watch list. In fact, *The Washington Post* reported on Sunday that our watch lists keep growing, with the Terrorist Identities Datamart Environment ("TIDE") - the master list from which other lists, like the No Fly list, are taken - now numbering about 435,000 people.

a. Doesn't such a large and constantly growing list actually make it harder for the FBI and others to use the information? Wouldn't the FBI and other agencies be able to do much more to protect us with a more controlled list, focused on serious and proven threats?

Response:

The FBI's counterterrorism watchlisting strategy is designed to enable law enforcement and screening personnel to effectively detect, disrupt, and/or assist national security components in tracking those suspected of involvement in terrorist networks. This strategy empowers Federal, State, local, and tribal security and law enforcement officials, who serve as "first preventors" in the global war on terrorism. The foundation of the FBI's counterterrorism watchlisting strategy is the requirement that the subjects of both preliminary and full-field investigations be watchlisted.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.071

The circumstances in which a preliminary or full-field counterterrorism investigation may be initiated are dictated by the October 31, 2003 AG Guidelines for FBI National Security Investigations and Foreign Intelligence Collection. Because the subjects of these investigations are automatically nominated for inclusion on the watchlist, the value and accuracy of the watchlist depend on the FBI's compliance with these AG Guidelines in initiating counterterrorism investigations. Other United States agencies that submit watchlist nominations are similarly required to ensure their nominations are made pursuant to appropriate guidelines. The Terrorist Screening Center (TSC) reviews all watchlist nominations to ensure they are adequately supported and meet Terrorist Screening Database (TSDB) criteria. The TSC also works hard to ensure that individuals are promptly removed from the watchlist as soon as it receives information indicating removal is appropriate.

It continues to be imperative that TSDB nominations be properly supported and that entries be promptly removed when errors occur or other circumstances warrant deletion. It is accuracy, far more than volume, that defines the value of the TSDB, and the FBI is committed to ensuring that our policies and practices ensure the greatest possible accuracy.

b. *The Washington Post* article also noted the difficulty that people on the list, or with names similar to people on the list, have in getting off of government lists -- which restrict their travel and their lives. The Government Accountability Office issued a report last year setting out some of the failures throughout the government in allowing individuals effective redress if they are wrongly placed on these lists. In light of the Arar situation, Senator Specter and I asked the Government Accountability Office to update their review. What steps has the FBI taken to allow individuals who may be wrongly on watch lists to challenge and correct those designations?

Response:

In January 2005, the TSC established a formal watchlist redress process. That process allows agencies using TSDB data during a terrorism screening process (screening agencies) to refer individuals' complaints to the TSC when it appears those complaints are watchlist related. The goals of the redress process are to provide for timely and fair review of individuals' complaints and to identify and correct any data errors, including errors in the TSDB itself.

The TSC has worked closely with screening agencies and others to develop a redress procedure that receives, tracks, and researches watchlist-related complaints and corrects inaccurate TSDB or other TSC data that is causing an individual hardship or difficulty during the screening process. While the terrorist

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.072

watchlist is an effective counterterrorism tool in large part because its contents are not revealed, and the redress process consequently does not inform individuals whether they are on the terrorist watchlist, the TSC's inability to provide transparency to affected individuals means the burden is on the government to perform a critical, in-depth review of the information supporting a person's inclusion in the TSDB to ensure it meets the watchlisting criteria. If sufficient information does not exist to justify a person's inclusion in the TSDB or its subsets (such as the No Fly List), the person will be removed. An enhanced redress process for individuals on the No Fly List provides for an administrative appeal of any adverse redress decision, the ability to request any releasable information, and the ability to submit information for consideration during the appeal.

Those who are misidentified as watchlisted can experience varying levels of difficulty when they fly or attempt to cross national borders. When these misidentified persons file redress complaints, review and any corrective actions are accomplished by the screening agency. The Government Accountability Office (GAO) recently completed a comprehensive review of the ongoing interagency efforts to improve the experience of misidentified persons (GAO Report 06-1031), including efforts by DHS to annotate their record systems to distinguish those persons more quickly in the future. The GAO Report highlights the TSC's significant efforts to improve the redress process and to assist misidentified persons, including a procedure for maintaining records of encounters with misidentified persons and for reviewing records when new encounters occur so the TSC can rapidly identify and clear known misidentified persons during screening. Information regarding the watchlist redress process and how to file a complaint with a screening agency is available to the public on the TSC's website at www.fbi.gov/terrorinfo/counterrorism/tsc.htm. Other agencies that use TSDB data for screening, including the TSA, also provide redress information on their websites.

SENTINEL

15. Now a year into the Bureau's Sentinel computer upgrade program, I remain concerned about the prospect of this program and its ballooning costs to American taxpayers. Earlier this month, the FBI informed the Committee that it had encountered unexpected problems with the deployment of Phase I of the Sentinel program that would delay the program. Even more troubling, the FBI could not tell Committee staff how long it would take to remedy these problems, or how the delay would impact the overall schedule for Sentinel.

a. What is the current status of the Sentinel program and do you anticipate that there will be additional delays in deploying the program or costs overruns?

These responses are current as of 7/31/07

38189.073

Response:

The FBI successfully deployed Phase 1 of the SENTINEL system to all Automated Case Support (ACS) system users worldwide on June 18, 2007, two months later than originally planned. Product integration problems and performance issues delayed delivery, and more testing was required to ensure fixes worked to specifications. In addition, the FBI changed the deployment approach to allow for a pilot period to test the system with actual users and ensure an accurate measurement of performance. The program was piloted in the Baltimore, Washington, and Richmond Field Offices and in one Division at FBIHQ. In addition to testing the system's functionality, the pilots also assisted in testing how the system handled the user load and in assessing the adequacy of the training materials.

The SENTINEL Program Management Office and Lockheed Martin prepared users for training and deployment, training nearly 250 field office and FBIHQ users as SENTINEL Training Advisors. This group assisted contract instructors in providing training and will continue to assist users in their divisions when questions arise.

The FBI deferred a total of 57 mostly low-level requirements from Phase 1 to later phases because they were outside of the scope of Phase 1, did not add value to Phase 1, required the modification of ACS, or would duplicate a capability included in a future phase. As a result of a series of contract modifications, some of which pre-purchased software for Phase 2, the cost for Phase 1 development, including award fees, increased from $57.2 million to $59.7 million.

b. What impact have the delays with Sentinel -- and Trilogy before it -- had on the Bureau's ability to fulfill its core mission?

Response:

The delays in updating the FBI's computer systems have had very little impact on the Bureau's ability to fulfill its core mission. All components of the FBI's ACS system have continued to be operational, and this information will be migrated to Sentinel. Phase 1 provides Sentinel's foundational base and enhanced access to the information contained in ACS. Phase 2 will bring the most new capabilities to the users, including automated workflow, document and record management, public-key infrastructure, digital signatures, and role-based access controls.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.074

CIVIL RIGHTS COLD CASES

16. In February 2006, the FBI established a nationwide initiative to re-examine civil rights era cold cases. At a press conference on February 27th, the FBI released a press statement announcing that although 100 cold cases have been referred to the Bureau, the FBI has prioritized only a dozen. I applaud the effort to reexamine these cases, but why has the FBI only prioritized a mere handful of civil rights era cold cases? How many agents, analysts, and other resources has the FBI committed towards this important effort?

Response:

While the FBI initially prioritized 10 cases for immediate assessment, all of the matters referred to the FBI as a result of this initiative have been forwarded to the 17 affected FBI field offices for preliminary investigation. Those offices will review available investigative files, court records, and public source information, determine if identified subjects and witnesses are still alive, and compile comprehensive witness and evidence lists. The facts of each case will be presented to both Federal and local prosecutors to assess possible prosecution potential, and matters identified as having both investigative and legal viability will be pursued. The FBI has 152 SAs assigned to work Civil Rights matters, including this important initiative.

17. Earlier this year, I joined Senator Dodd in re-introducing the Emmett Till Unsolved Civil Rights Crime Act. This bill creates permanent unsolved civil rights crimes units within the FBI and the Civil Rights Division of the Justice Department to investigate and prosecute these crimes. This bill will also give law enforcement the resources to ensure that justice is served. As a former prosecutor, I strongly believe law enforcement should have the necessary tools to aggressively seek those who have committed these crimes, regardless of the time that has passed. Would you support the Emmett Till bill? Do you believe this bill gives the FBI the resources needed to thoroughly investigate unsolved civil rights murders?

Response:

As indicated during the testimony of Deputy Assistant AG Grace Chung Becker in a June 12, 2007 hearing before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, DOJ and the FBI support the goals of the Emmett Till Unsolved Civil Rights Crimes Act, but have offered recommendations to improve its effectiveness.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.075

LOST LAP TOPS/ DATA SECURITY

18. In February, the Inspector General for the Department of Justice released another troubling report finding that the FBI lost 160 laptop computers - including at least ten computers that contained classified information and one that contained sensitive personal information about FBI personnel - during a 44-month period. Even more troubling, the report also found that the FBI could not even account for whether 51 other computers, including seven computers that were assigned to the Bureau's counterintelligence and counterterrorism divisions, might contain classified or sensitive data. What is the Bureau doing to address its problem of lost laptops and lax data security?

Response:

The DOJ OIG recognizes that the FBI has made substantial progress since the OIG initiated its review. The report itself states that "the FBI has made progress in decreasing the rate of loss for weapons and laptops" and notes the positive trend in this direction since the FBI's implementation of corrective actions in 2002. This progress reflects the FBI's commitment to minimizing such losses. The statistics cited in the report reflect a substantial reduction in the average number of laptops lost or stolen in any given month when compared to information in the 2002 OIG report. The report additionally recognizes that "in an organization the size of the FBI, some weapons and laptops will inevitably be stolen or go missing."

The FBI recognizes that more needs to be done to ensure the proper handling of laptop computers (and the information on these laptop computers) to minimize the incidents and ramifications of loss and theft. One of the most important steps to ensuring the security of the information on our laptop computers is the encryption and password protection of this information. To this end, the FBI requires that all FBI laptops be configured to include encryption that protects the sensitive but unclassified information they may contain, such as personally identifying information (PII). The policy requiring this configuration contains a total of nine requirements and recommendations designed to minimize the potential for loss of FBI laptops and information. Additional policies related to the protection not only of PII but also of other information, including National Security information, were promulgated in April 2006 and articulated in the FBI's comprehensive Security Policy Manual.

19. Earlier this year, Senator Specter and I reintroduced our Personal Data Privacy and Security Act, which would, among other things, require federal agencies to give notice to the individuals whose data is lost or stolen, when a data breach occurs. Did the FBI notify

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.076

the individuals whose sensitive personal information was lost in the case of the missing laptops? Would you support this legislation?

Response:

The FBI bases its response to a compromise of PII on the circumstances of the breach. In appropriate cases, the affected individuals are notified. However, in some cases notice is deemed unnecessary because the risk of data compromise is almost non-existent (e.g., where an effective security system blocks access to data), in some cases notice may compromise a criminal or national security investigation, and in some cases notice is not possible because there is no way to determine which identities were compromised. The FBI is in the process of developing a formal data breach policy that will comport with guidance provided by the Office of Management and Budget (OMB). The FBI has not taken an official position regarding the Personal Data and Security Act and will defer to DOJ in this regard.

20. After the VA lost a lap top containing sensitive personal information about millions of veterans and active duty personnel, Secretary Nicholson instituted a new policy requiring that all of the VA's computers contain encryption technology to prevent the unauthorized disclosure of sensitive information. Will you make a similar pledge to use encryption technology for all of the Bureau's computers?

Response:

The FBI's security policy requires that FBI-owned and FBI contractor-owned laptop computers used for FBI work be equipped or configured according to Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," or with National Security Agency-approved encryption if the laptop contains FBI information (including Classified, Sensitive But Unclassified, For Official Use Only, or Law Enforcement Sensitive information), operates in other than a stand-alone mode, or connects to the Internet.

DNA SAMPLING

21. Pursuant to a little noticed provision in the Violence Against Women Act reauthorization bill, the Department of Justice is currently developing new guidelines that would greatly expand the Government's ability to collect DNA samples - which reveal the most sensitive genetic information about an individual - from most individuals who are arrested or detained by federal authorities and to store this sensitive biological information in a federal data base known as the National DNA Index System. This new policy will

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.077

allow the Federal Government to collect DNA samples from hundreds of thousands of illegal immigrants who may be detained by federal authorities and from individuals who may be arrested - in essence, making DNA collection as common as fingerprinting. What privacy protections are in place under the Department's new guidelines to ensure that sensitive DNA data contained in the National DNA Index System will not be misused or improperly disclosed by the FBI or other federal and state agencies?

Response:

While the FBI is working with DOJ to finalize the regulations on DNA sample collection relative to Federal arrestees and detainees, there are already a number of protections in place and they are vigorously enforced. When arrestee and detainee DNA samples are collected, they are placed in the National DNA Index System (NDIS) offender database. The offender and crime scene databases are populated by profiles from Federal, State, and local law enforcement agencies. The profiles within the database use only genetic markers that provide identification; no other genetic information, such as medical status, can be gleaned from these markers, and NDIS, which is in essence a pointer system, does not contain any names or personally identifying information. Instead, each profile is associated with a unique identifier that traces back to the laboratory that developed that particular profile and placed it in the database. Once a "hit" occurs and is confirmed, then the two laboratories involved will exchange information regarding the individual involved.

Although all states participate in NDIS, they do not have direct access to the national database. NDIS is searched once a week at the FBI and a hit report is generated. If an individual lab desires to follow up on a particular hit (generally the lab that contributed the forensic sample), it contacts the laboratory that provided the offender information and a confirmation process begins. During that process, the laboratories follow written procedures to ensure the hit is related to the correct offender; these procedures include re-working a portion of the remaining sample and re-comparing results. Under procedures established by the NDIS Board, no names or other personally identifying information may be reported until the confirmation process is complete.

Federal law also provides privacy protections, including criminal penalties for privacy violations. By law, NDIS DNA information must be

> [m]aintained by Federal, State, and local criminal justice agencies (or the Secretary of Defense in accordance with section 1565 of Title 10) pursuant

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.076

> to rules that allow disclosure of stored DNA samples and DNA analyses only –
> (A) to criminal justice agencies for law enforcement identification purposes;
> (B) in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
> © for criminal defense purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged; or
> (D) if personally identifiable information is removed, for a population statistics database, for identification research and protocol and development purposes, or for quality control purposes.

(42 U.S.C. § 14132(b)(3).) These protections are further bolstered by provisions that reiterate these protections and provide criminal penalties for individuals who knowingly disclose DNA information from the database to a person or agency not authorized to receive it. (See, for example, 42 U.S.C. § 14133© and 42 U.S.C. § 14135e©.)

22. I am also concerned about this new policy because the new DNA evidence collected by the Government will add to the already notorious backlog at the Bureau's laboratory. According to press reports, the FBI acknowledges that this new policy will result in an increase of as many as 1 million additional DNA samples a year. Is the Bureau's laboratory equipped to handle this additional workload? What steps are you taking to make sure that the FBI's laboratory can keep up with the demand for DNA samples?

Response:

The FBI's Federal Convicted Offender (FCO) Program is responsible for collecting and processing DNA samples collected from those convicted of Federal felonies for the purpose of retention and cataloging in the FBI's National DNA Database. The FCO Program receives samples from over 500 collection sites across the country. Since the program's inception in June 2001, over 225,000 samples have been received, with 7,000 to 8,000 samples currently received monthly. To date, the FCO Program has uploaded over 34,000 samples into the National DNA Database, resulting in over 600 hits. While the volume of sample submissions to the FCO Program has increased dramatically since 2001, the FBI Laboratory has received no additional resources to support this work.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.079

While much of the DNA analysis process has been automated, the volume of sample submissions to the FCO Program has increased dramatically since 2001. A bottleneck continues to exist at the DNA data review stage, which is currently conducted manually. To alleviate this bottleneck, the FBI is evaluating data analysis software packages and expert systems to automate this part of the process. Once implemented, the resulting system would be able to assess 85 percent to 90 percent of the convicted offender data without manual intervention, reducing data analysis time from approximately 60 minutes (per 80 samples) to less than 15 minutes. The FY 2008 budget request also includes $15 million to address the workload increases for the FCO Program.

IMPROPER REPORTING OF TERRORISM STATISTICS

23. The Department of Justice Inspector General found in another recent report that the FBI failed to accurately report eight of the ten terrorism statistics that it reviewed for this report - that is an 80% failure rate. Among other things, the FBI overstated the number of terrorism-related convictions for 2004, because it included cases where no terrorism link was actually found. This is no simple matter -- the Congress relies upon these statistics to conduct oversight and to make funding and operational decisions regarding the Bureau. What steps have you taken to address the problems with reporting of terrorism statistics at the FBI?

Response:

The FBI has modified and substantially improved the systems and internal controls related to terrorism reporting. Following the attacks of September 11, 2001, the FBI underwent a substantial reorganization and restructuring, and many of the apparent weaknesses in statistical reporting discussed in the OIG report entitled, "The Department of Justice's Internal Controls over Terrorism Reporting" occurred during, and were a result of, that reorganization and restructuring. The backbone of the FBI's statistical reporting system is the case management system, along with its supporting information technology systems. These systems were not originally designed to capture or report on the enhanced requirements developed as part of the FBI's post-9/11 reorganization and restructuring. The FBI recognized this challenge in 2002 and began a concentrated effort to build supporting systems that include additional internal controls to ensure that we accurately capture and report on the activities involved in our post-9/11 intelligence mission. The FBI has made significant progress in the development and implementation of these systems, which are being upgraded as part of the FBI's Sentinel project.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.080

Also since the time period examined by the OIG Report, the FBI has made significant strides in the development of a new central management information system known as the Comprehensive Operational Management Plan Advancing Specific Strategies (COMPASS). COMPASS accumulates statistical accomplishments from various stand-alone systems and presents the information in a unified format available to all senior managers both at FBIHQ and in FBI Field Offices. COMPASS is one example of the FBI's commitment to improving and sharing statistical reporting with FBI senior managers. The bulk of the information captured in COMPASS is used internally to identify trends and to evaluate progress against the FBI's defined strategic objectives. The FBI continues to make extensive efforts to refine performance metrics that measure the FBI's achievements against strategic outcomes.

STAFFING

24. I also remain concerned about staffing at the Bureau. In January, your Deputy, John Pistole, told the Senate Intelligence Committee that the FBI expects to lose 400 agents and 400 intelligence analysts this year, due to retirement or attrition. Mr. Pistole also stated that approximately 20% (370) of the FBI's intelligence analysts have less than a year of experience with the Bureau. I cannot help but worry that the Bureau will not have the staffing and expertise that it needs to carry out its counterterrorism and counter-intelligence mission, given these figures on staffing. What are you doing to address the shortage in intelligence analysts and agents? How many agents and analysts do you expect to hire by the end of 2007?

Response:

The FBI's top priority for Fiscal Year (FY) 07 was to recruit highly qualified, diverse applicants targeting specific critical skills and backgrounds, including foreign languages, intelligence, computer science/information technology, accounting/finance, engineering, law enforcement/law/military, and science.

The FBI employs several recruitment strategies to support the recruitment of SAs, IAs, language analysts, and others possessing critical skills and backgrounds, including minorities, women, and those with disabilities. The most effective strategies have included the following.

- National advertising, including television, radio, Internet, billboards, airport dioramas, and print media.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.081

- Participation in over 900 national and local targeted career fairs and conferences annually to maximize the FBI's access to high-quality, diverse applicants with critical skills.

- Partnering with diverse organizations such as the U. S. Copts' Association, American-Arab Anti-Discrimination Committee, Sikh Foundation of Virginia, Sikh Council on Religion and Education, Kaur Foundation, Intelligence Analyst associations, National Society of Black Engineers, Black MBA Association, American Arab Institute, and U. S. Arab Economic Forum.

- Targeted intern and co-op programs.

- Continuation of the FBI's EdVenture Partners Collegiate Marketing Program.

- Expanded partnership with the Faith-Based Council on Law Enforcement and Intelligence.

- Using recruitment contractors whose missions focus on the recruitment of applicants possessing such expertise as intelligence, foreign languages, information technology, and middle eastern cultures.

- Featuring onboard employees with critical experience and education in line with the FBI's targeted hiring goals and objectives in all new recruitment media (such as advertisements, brochures, exhibits, and videos), clearly demonstrating the FBI's diversity.

- Continued participation in the Intelligence Community Recruiting Group, which meets monthly, includes all recruitment chiefs in the Intelligence Community (IC), and engages in joint recruitment, training, and diversity seminars.

The FBI's Hiring Plan provides for the addition of 287 SAs and 112 IAs in FY 2007. We have been successful in recruiting IAs with the specialized skills needed to build our Intelligence Program, hiring 1,448 IAs in the past 3 years, including a mix of IAs who have either specialized skills that target specific knowledge or general analytic skills. In order to recruit and hire IAs with the skills and educational backgrounds needed to meet our national security mission, the FBI developed a targeted recruitment strategy that identifies the critical skills required by the FBI to satisfy its current mission as well as those needed to address the organization's future challenges. The FBI is updating the recruitment

---

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.082

strategy to reflect the current hiring environment for the intelligence workforce and anticipates releasing a modified version of this strategy by the end of 2007.

25. I was disappointed to learn that the FBI has not met several of its goals to improve FOIA processing under the President's Executive Order 13,392, including the important goal to complete all FOIA requests that are more than two years old by August 2006. What is the current status of the FBI's FOIA backlog?

Response:

The FBI identified 24 goals designed to improve our efficiency in processing requests under the Freedom of Information Act (FOIA), the professionalism of staff employees, and customer service, establishing an ambitious multi-year plan for implementing these improvements. The FBI met its interim and completion targets with respect to all but eight goals, and continues to work on these remaining goals.

Despite a 40 percent increase in FOIA requests (from 10,873 in FY 2005 to 15,349 in FY 2006), the FBI met or surpassed its goals related to the time required to process requests. The median time for processing small requests (those of less than 500 pages) decreased by 10 percent (the goal was a 10 percent reduction) and the median time for processing medium requests (500 to 2499 pages) decreased by 16 percent (this goal was also a 10 percent reduction). The median time required to process all pending requests decreased by 36 percent (the goal was a 20 percent reduction).

Although not among our designated goals because of the difficulty in predicting the volume of incoming requests, we also worked hard to reduce the number of requests pending at any given time. Overall, we reduced the number of pending requests from 1,796 at the end of FY 2005 to 1,750 at the end of FY 2006. This included a 58 percent reduction in the number of pending large requests (those of 2,500 pages or more) from the end of FY 2005 to the end of FY 2006 (a reduction from 122 to 51), and this number continued to decrease, with 42 requests pending on April 1, 2007. The number of pending medium requests also decreased, from 691 at the end of FY 2005 to 203 on April 1, 2007, with a corresponding decrease in the median amount of time for which medium requests were pending (from 556 days at the end of FY 2005 to 273 days on 4/1/2007).

Contrary to the indication in the question, the FBI's goal was not to "complete all FOIA requests that are more than two years old by August 2006." The FBI's goal was to "continue emphasis on completing requests over two years old." Even before development of the FBI's Improvement Plan, the FBI had identified 74

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.083

requests (approximately 320,700 pages) received by the FBI before August 14, 2003 and was developing a plan to complete them. The FBI successfully met its August 15, 2006 interim goal of developing a plan for processing older requests. As of September 1, 2007, 72 of these requests had been closed by reviewing 290,300 pages. As part of the continuing emphasis on requests over two years old, on August 15, 2006 the FBI identified 36 pending requests (an estimated 72,000 pages) received between August 15, 2003 and August 15, 2004. As of September 1, 2007, 34 of these requests had been closed by reviewing 68,670 pages. The FBI continues to both process and provide interim releases with respect to the remaining open requests.

26. After the horrific attacks of September 11th, I worked very hard with others in Congress to give the FBI the tools that it needed to combat terrorism and carry out its domestic intelligence functions. Given what we have learned about the widespread misuse of National Security Letters and chronic staffing problems in the Bureau's counterterrorism and counterintelligence offices, some are calling for the Congress to put the Bureau's domestic intelligence operations in a new MI5-styled domestic intelligence agency. Do you believe that Congress should create a domestic intelligence agency to carry out the Nation's domestic counterterrorism activities?

Response:

The FBI believes there is no reason to separate the functions of law enforcement and domestic intelligence, as would occur if the MI-5 model were adopted. On the contrary, combining law enforcement and intelligence affords us ready access to every weapon in the government's arsenal against terrorists, allowing us to make strategic and tactical choices between the use of information for law enforcement purposes (arrest and incarceration) or intelligence purposes (surveillance and source development).

The benefits of this approach have been clearly borne out. Since September 11, 2001, the FBI has identified, disrupted, and neutralized numerous terrorist threats and cells, and we have done so in ways an intelligence-only agency like the United Kingdom's MI-5 cannot.

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

- A worldwide network of highly trained and dedicated SAs;
- Intelligence tools to collect and analyze information on threats to national security;

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.084

- Law enforcement tools to act against and neutralize those threats;
- Expertise in investigations and in the recruitment and cultivation of human sources of information;
- Longstanding and improving relationships with those in state and local law enforcement, who are the intelligence gatherers closest to the information we seek from these communities; and
- Nearly a century of experience working within the bounds of the United States Constitution.

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

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

Both the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) and the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) agree that the FBI should retain its domestic intelligence responsibility. Similarly, in its March 2005 report entitled, "Transforming the FBI: Progress and Challenges," a panel of the National Academy of Public Administration wrote: "This Panel, like the 9/11 Commission, is convinced that the FBI is making substantial progress in transforming itself into a strong domestic intelligence entity, and has the will and many of the competencies required to accomplish it. That Panel recommended that the FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counterintelligence, cyber, and transnational criminal activity."

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.085

The WMD Commission also examined the FBI's intelligence program and concluded in March 2005 that it had been significantly improved since September 11, 2001. The commission rejected the need for a separate agency devoted to internal security without any law enforcement powers, recognizing that the FBI's hybrid intelligence and investigative nature is one of its greatest strengths and emphasizing the importance of the ongoing effort to integrate intelligence and investigative operations. At the same time, the commission noted that the FBI's structure did not sufficiently ensure that intelligence activities were coordinated with the rest of the IC. Accordingly, the commission recommended the creation of a "National Security Service." In response to the President's directive endorsing that recommendation, the FBI created the National Security Branch, which combines under one leadership umbrella the capabilities, resources, and missions of the Counterterrorism Division, Counterintelligence Division, Directorate of Intelligence, and WMD Directorate. The structure offered by the National Security Branch ensures the integration of national security intelligence and investigations, promotes the development of a national security workforce, and facilitates a new level of coordination with our partners in the IC.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.086

Questions Posed by Senator Kennedy

27. The Hate Crime Statistics Act requires the Justice Department to publish an annual summary of crimes which "manifest prejudice based on race, religion, sexual orientation, disability, or ethnicity," based on data from law enforcement agencies across the country. In 2005, there were 7,163 such crimes. 3,919 were motivated by racial bias; 1,227 by religious bias; 1,017 by sexual orientation bias; 944 by ethnicity/national origin bias; and 53 against disabled individuals. 12,417 law enforcement agencies in the United States participated in this data collection effort. Only a small percentage of law enforcement agencies in the nation participated, and only 16% of the participating agencies reported even a single hate crime.

a. What steps is the FBI currently taking to increase participation in the data collection effort?

Response:

The FBI's hate crime data collection effort is part of the Uniform Crime Reporting (UCR) program, which is a nationwide, cooperative statistical effort that depends on the voluntary reporting of Federal, state, tribal, city, county, and university law enforcement agencies. In 2005, the reporting agencies represented more than 245 million inhabitants, or 82.7 percent of the nation's population, including reporting from 49 states (hate crime information is not received from Hawaii) and the District of Columbia. Though the published 2005 UCR statistics did not include hate crime data for New York City or Phoenix, the FBI's UCR program has worked with these cities and has obtained their data for inclusion in the 2005 hate crime database.

The UCR program relies on the good faith reporting by its participating agencies of bias-motivated crime. Periodically, the UCR program forwards to state UCR program managers quality reviews that identify reported hate crimes by reporting agency, listing those agencies for which no information is received. At that time, the FBI encourages the submission of any missing or incomplete information. The UCR program has strongly endorsed the collection of hate crime statistics in electronic format. Currently, 73 percent of the hate crime statistics are submitted in electronic format, typically by using the National Incident-Based Reporting System (NIBRS) and interactive online communications through Law Enforcement Online (LEO).

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.087

b. How much training is the FBI currently providing to state and local law enforcement authorities to improve identification, reporting, and response to hate crimes nationally?

Response:

The FBI's UCR program provides training materials in print, online, and, when funding permits, on site for the agencies that request it. During the last three fiscal years, the FBI's UCR program has provided almost 6,000 printed hate crime training manuals to law enforcement. In addition, the UCR program has conducted on-site training for 63 agencies regarding issues specific to hate crimes, and web-based hate crime training is available to law enforcement through LEO. The UCR program also provides training regarding hate crime reporting when it trains law enforcement personnel regarding Summary reporting and NIBRS. UCR program contributors and stakeholders are informed of hate crime reporting procedures and training opportunities through the UCR *State Program Bulletin* and *UCR Newsletter*, among other means.

28. Attached is a June 26 letter signed by 42 national civil rights, law enforcement, civic, and religious organizations which includes recommendations, prepared in response to the 71 FR 24869 request for comments on improving the Act. In meetings with government officials and community-based organizations, FBI representatives have indicated that an interagency hate crime working group was created to revise and update FBI resources under the Act.

a. What is the current status of this Hate Crime Working Group?

Response:

Former Attorney General Reno convened a Hate Crime Working Group at DOJ in May 1997. The Working Group was initially chaired by David W. Ogden, Counselor to the Attorney General, and met approximately weekly. Members of the Working Group included interested components throughout DOJ and the FBI. The Working Group examined five principal areas related to hate crime: legislative initiatives, data collection, community outreach, prosecution and enforcement, and coordination. The Working Group developed a number of specific recommendations, including the formation of local hate crime working groups in Federal judicial districts under the leadership of or with the participation of each U.S. Attorney's Office. The local working groups were envisioned as including local community leaders and educators, as well as Federal, State, and local law enforcement officials, and were to be the primary mechanism for evaluating and addressing the hate crime problem in the local community.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.088

The FBI defers to DOJ regarding the current status of this Working Group.

b. What is the status of plans to revise and update the FBI's Hate Crime Incident Report forms to provide space to encourage additional narrative about the bias motivation?

Response:

The UCR program is evaluating the current Hate Crime reporting program and exploring opportunities for program enhancement, including the possible inclusion of narrative comments or structured narrative fields. This evaluation must include consideration of how to ensure the value of subjective, unstructured narrations and how to limit the burden on those drafting the narratives to accurately and succinctly depict incidents. Once the FBI has evaluated this issue, recommendations will be provided to the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) for review and recommendation to the FBI Director.

c. What is the status of plans to revise and update the Bureau's 1999 training materials on how to identify, report, and respond to hate crimes to reflect post-9/11 realities?

Response:

The FBI is reviewing all training materials, including both hard copy and web-based materials, to ensure law enforcement has the tools it needs to accurately and efficiently report hate crimes. Recommendations based on this review will be presented to the CJIS APB to ensure consensus within the law enforcement community.

29. Attached is an exchange of letters between 51 national organizations and your office. On October 23, 2006 these groups wrote to you to express concerns that the 2005 edition of the comprehensive FBI crime data compendium, *Crime in the United States,* was published without a summary of hate crime data for the first time since 1996. The FBI Assistant Director in charge of the Criminal Justice Information Services Division, Thomas E. Bush, III, responded in the attached November 30 letter, stating:

> **"Although the decision to exclude preliminary hate crime data from *Crime in the United States* was well thought out and thoroughly reviewed, we understand the concerns expressed in your letter. In response, the FBI will work to better align hate crime statistics with *Crime in the United States,***

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.089

***2006,* thus giving hate crime data more visibility in conjunction with this publication."**

What is the status of efforts to integrate data from the Act into *Crime in the United States, 2006?*

Response:

A link to hate crime statistics is provided on the main navigation page of the electronic version of the UCR (www.fbi.gov/ucr/ucr.htm). This link connects to the hate crime statistics for the selected year.

30. Professor Jack McDevitt, Director of The Center for Criminal Justice Policy Research at Northeastern University in Boston, has emphasized the need for an expanded narrative in reporting hate crimes. In his September 2002 report, *Improving the Quality and Accuracy of Bias Crime Statistics Nationally,* funded by the Justice Department's Bureau of Justice Statistics, Professor McDevitt suggested that more detailed reporting can reduce the occurrence of "information disconnect" between the investigating officer and Uniform Crimes Report reporting officials.

The current reporting form provides boxes only for "Anti-Hispanic" and "Anti-Other Ethnicity." In light of the disturbing number of post-9/11 "backlash incidents" in the aftermath of the September 11th terrorist attacks, do you believe that the form should include additional boxes for "Anti-Arab," "Anti-Muslim," and "Anti-Sikh" crimes, among others?

Response:

The FBI's UCR program collects hate crime data in accordance with the Hate Crime Statistics Act of 1990, as amended, and in compliance with the standards for race and ethnicity designations established by OMB. The current Hate Crime Incident Report Form collects "Anti-Islamic (Muslim)" data under the category of "religious bias motivation." The FBI recognizes the possible value of establishing separate categories for "anti-Arab" and "anti-Sikh," but there is no current consensus on how to define these terms (for example, should they be based on geography, culture, religion, or native language). Therefore, absent a consensus on definitions for these categories, the FBI does not intend to include "Anti-Arab" or "Anti-Sikh" bias motivation types.

31. As states continue to enact hate crime statutes, the clear trend has been to include gender-based crimes in these laws. In 1990, only seven of the statutes in the thirty-one states with hate crime laws included gender. Today, including the District of Columbia,

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.090

twenty-eight of the forty-five states with penalty-enhancement hate crimes statutes include gender-based crimes. Eight states now include gender in their hate crime data collection mandate. Gender-based crimes are subject to federal sentencing enhancements under 28 U.S.C. § 994.

a. Do you believe that the FBI's Hate Crime Incident Report should include a box in the Bias Motivation section for gender-based hate crimes?

b. Is there a legal impediment to making that change, or could the Bureau take this step on its own?

Response:

The categories of bias reported in the UCR are based on the Hate Crime Statistics Act of 1990, as amended, and OMB's minimal standards for race and ethnicity designations. While the FBI does not anticipate revising the bias motivation categories absent revision of these authorities, there is no legal impediment to seeking additional voluntary reporting from law enforcement. If the FBI were to contemplate this, we would seek consideration of the proposal by the CJIS APB.

32. In your March 9, 2007 press conference after the release of the Inspector General's report, you were asked if any FBI personnel would face criminal sanctions for their conduct relating to the FBI's misuse of its National Security Letter authority. You said the IG report found no criminal misconduct, so your inspection division review of this matter is "to determine whether or not there should be any administrative actions taken." When questioned again you actually quoted from page 124 of the IG report, where the IG stated "we also did not find any indication that the FBI's misuse of NSL authorities constituted criminal misconduct." But the IG backed off from this definitive statement in his congressional testimony in the House of Representatives last week, saying "we did not do a thorough review of what people up and down the line knew and did," and later that "we didn't do a review where we asked each individual, "What did you do and why?" The IG suggested that you were going to conduct that sort of review: "The FBI is looking at the evidence right now to see what people knew and what they did." Since you now know that the IG didn't look for criminal misconduct during his audit, will you expand your review to investigate the possibility of criminal misconduct?

Response:

On March 9, 2007, the FBI Director directed the Inspection Division to thoroughly investigate concerns raised by the DOJ OIG. Thereafter, the OIG announced it would initiate a review of the FBIHQ unit in question. The Inspection Division is working jointly with the DOJ OIG in its review, with

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.091

DOJ's OIG designated as the lead agency. In addition, former Attorney General Gonzales asked an Associate Deputy Attorney General and DOJ's OPR to examine the role FBI attorneys played in the use of exigent letters. The FBI Director will review the results of all such inquiries when available and take appropriate action.

33. In fact, there is ample evidence that this misconduct was intentional. The Inspector General's report confirms that the Office of General Counsel knew of the FBI's misuse of National Security Letter authorities. In fact, OGC was put on notice of problems with NSLs a[s] late as 2004, yet did nothing to stop the abuses and in some cases, sanctioned them:

a. At least one OGC procurement attorney reviewed contracts between the Communications Analysis Unit and three phone companies, which were the basis for illegal "exigent" letters (p. 88-89);

b. Field agents complained about improper Communication Analysis Unit requests to the OGC's National Security Law Bureau as long as two years ago (p. 93);

c. NSLB attorneys gave improper advice to the Communications Analysis Unit and told them it was proper to issue exigent letter in true emergencies, despite any statutory grant to do so (p. 93);

d. NSLB attorneys discovered they were misled by Terrorist Financing Operations Section supervisors on the use of "Certificate Letters," yet the letters continued to be used[;]

e. FBI lawyers in the field, Chief Division Counsels, reported that they felt intimidated by their Special Agents in Charge and would approve NSL requests when they would have preferred to reject them out of fear of challenging their Special Agents in Charge.

Are you concerned that FBI attorneys were so intimately involved in this illegal conduct and allowed it to continue despite their reservations? Doesn't the involvement of attorneys in this misconduct make the illegal activity appear intentional? Have you reported these attorneys to the bar?

Response:

Without concurring with the premises or asserted factual representations within this question, please see the response to Question 32, above. The FBI Director

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.092

will review the results of the referenced inquiries when available and take appropriate action.

34. FBI General Counsel Valerie Caproni also testified before the House of Representatives last week. In response to questioning about the inability of the FBI to tie the use of NSLs to criminal terrorism prosecutions, Ms. Caproni said that "It is my belief that virtually every counterterrorism case that began in its normal course of affairs is likely to have a national security letter used sometime during it."

a. Does that mean every FBI terrorism prosecution used evidence obtained with NSLs? If this is so, why can't the FBI demonstrate it with data supporting this claim?

Response:

NSLs, which are an essential tool in national security investigations, are used to obtain basic information for use in national security investigations, similar to that routinely obtained through grand jury subpoenas for use in criminal investigations. Just as no prosecutor or investigator tracks the usefulness of grand jury subpoenas in criminal investigations or prosecutions (although all would say grand jury subpoenas for documents can be critical to investigations), the FBI has not tracked the usefulness of NSLs in national security investigations. Moreover, while some national security investigations ultimately result in criminal prosecutions, disruption through arrest is only one of many appropriate responses the FBI may have to a national security threat.

b. Has evidence obtained with NSLs been entered into evidence in any criminal proceeding? Was the fact that the evidence was obtained with an NSL disclosed to the court, or to defense counsel?

Response:

It is certainly possible that records initially obtained through the service of NSLs have been introduced into evidence during criminal trials. There is no legal obligation to disclose the manner in which documents are obtained before introducing them in evidence. See, for example, Federal Rule of Criminal Procedure 16.

c. If evidence obtained with NSLs is used to support wiretap requests or search warrants, is that fact disclosed to the defense counsel at trial, and does the defense counsel have an opportunity to challenge that evidence for legal insufficiency?

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.093

Response:

Generally, the means used to obtain evidence that is used to support a wiretap request or a search warrant is not disclosed to defense counsel as a part of normal criminal law discovery practice. However, a criminal defendant always has the opportunity to challenge the sufficiency of incriminating evidence introduced by the prosecution at trial. A criminal defendant also may contest the *legality* of a search or seizure of evidence under the Fourth Amendment. And, as a statutory matter, a defendant also may challenge the legality of certain surveillance activities that are within the scope of either Title III or the Foreign Intelligence Surveillance Act (FISA). It should be noted, though, that records obtainable by an NSL are third-party records in which individual customers have no constitutionally protected privacy interest (see *United States v. Miller*, 425 U.S. 435 (1976); see also *Smith v. Maryland*, 442 U.S. 735 (1979) and which are not covered by either Title III or FISA. Therefore, we believe it is unlikely that a criminal defendant would be successful in suppressing a wiretap or search because it was based in some fashion on information obtained through an NSL.

d. Can you assure Congress that no evidence obtained with an "exigent letter" or with an improper or illegal NSL request was ever used in evidence in any criminal proceeding, or used to support a search warrant or wiretap that was later used as evidence?

Response:

Please see the responses to Questions 6 and 34c, above.

35. General Counsel Caproni also said she could not confirm any instance in which information gathered with NSLs was used to prevent a terrorist attack. Can you confirm such an instance? Why should Congress accept that NSLs are "indispensable," when no data support such a claim?

Response:

Just as it would be difficult to demonstrate that information obtained through a grand jury subpoena had been used to prevent a murder, it is difficult to point to the use of an NSL to prevent a terrorist attack. NSLs are used to gather very specific types of third-party records that are used to identify and understand the adversaries who seek to do us harm. Once this information is obtained, other investigative tools may be used to disrupt the plans of terrorists, saboteurs, and spies.

These responses are current as of 7/31/07

38189.094

For example, during the investigation of a terrorist financier and recruiter, NSLs for financial records and telephone toll billing records helped the FBI identify banks and accounts that were used to facilitate his terrorist fund-raising efforts. He was eventually identified as having provided instructions for terrorist activities in the United States. Although this financier and recruiter was not prosecuted, he was deported based upon the information developed during the investigation - information attributable in part to the information received through the use of NSLs.

In another case, the FBI received information from a foreign government indicating that individuals using e-mail addresses in the United States were in contact with an e-mail address belonging to a suspected terrorist. The FBI served NSLs on the relevant Internet service providers, and the investigation that followed indicated that these individuals were involved in plots against the United States, leading to indictments on various terrorism-related charges.

36. A March 20, 2007 Washington Post article suggested that the FBI will continue to use "emergency" requests to obtain records in advance of issuing NSLs or grand jury subpoenas.

a. Under what authority would the FBI use an emergency request?

Response:

Emergency disclosures are authorized by 18 U.S.C. § 2702(c)(4), which provides that an electronic communications service provider may voluntarily disclose to a governmental entity a record or other information (other than the contents of communications) pertaining to a subscriber or customer if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay. Pursuant to this provision, the FBI may present a service provider with information indicating the existence of an emergency and ask the provider to produce records or other non-content information in accordance with the provisions of the statute, recognizing that the statute authorizes the provider to make the determination and that production of the requested information would be voluntary on his or her part. A good example of when such a need might arise is as follows. Suppose a child is kidnapped, her parents receive a ransom call, and their telephone's caller ID function identifies the telephone number from which the ransom call was placed. In that circumstance, the FBI has a need to obtain telephone information immediately, but the facts underlying the emergency circumstance are unknown to the

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.095

telephone company at that point. Pursuant to section 2702(c)(4), if the FBI provides the facts to the telephone company, that company may provide the requested records if it decides that those facts justify an emergency disclosure of customer records. Such a need could also arise in the national security arena. Suppose, for example, the FBI receives a call anonymously warning that a bomb has been placed in the Sears Tower. The FBI would want to immediately identify the individual who placed the call and to determine others to whom the caller is related. That investigation would start by quickly gathering the telephone records of the telephone from which the anonymous call was placed.

b. The article said that under FBI policy, these requests could even be oral. Is there such a policy? Given what we have learned about the FBI's mismanagement of the NSL authority, and the lack of internal controls, why is it appropriate to use oral requests for documents?

Response:

An oral request would be entirely appropriate in an emergency in which delay could endanger lives. FBI policy requires documentation of the basis for an oral request and the service provider's response "forthwith." FBI policy also requires approval by an Assistant Special Agent in Charge (ASAC) in the field or a Section Chief at FBIHQ before a service provider may be asked to consider voluntarily disclosing the requested information pursuant to these provisions. Examples of when an oral request would be appropriate include the examples discussed above.

c. How does the FBI define an "emergency" as it pertains to a request for documents? What are the criteria? Is this a written policy, or does each agent decide on his own whether an emergency exists?

Response:

The statute requires "an emergency involving danger of death or serious physical injury to any person" requiring disclosure without delay. The FBI has not further defined this language. Under FBI policy, as indicated in the preceding response, a judgment call about whether to present information concerning such an emergency to an electronic communications service provider would be made by ASACs in FBI field offices or Section Chiefs at FBIHQ. Ultimately, the statute requires the service provider, with the information provided by the FBI, to make a good faith determination whether there is an emergency that justifies its voluntary release of this information.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.096

37. The FBI has no policy on retention of improperly collected records, and does not require the purging of records of individuals proved not to be linked to terrorism.

a. Why was there no guidance to field agents on when or how to store and access information before November 2006?

Response:

The FBI has long had a records management plan, approved by the National Archives and Records Administration, for general record keeping. All FBI files are subject to a record-keeping plan which, among other things, provides for the preservation or destruction of records under specified circumstances. Materials obtained pursuant to NSLs were treated no differently than documentary materials obtained pursuant to other legal processes.

b. Field agents were asking for guidance on ad hoc basis, so the Office of General Counsel knew there was confusion in the field. Why didn't you develop a policy?

Response:

As noted above, there was a general records keeping plan in place and, as noted below, policies were developed as the need arose.

c. Why was an OGC guidance issued in November 2006? Was the guidance issued to mute the IG's criticism?

Response:

The issuance of guidance in November of 2006, which relates to the reporting of potential IOB matters, was not tied to any particular event. Since September 11, 2001, the mission of the FBI had expanded exponentially in the intelligence arena, and large numbers of FBI personnel were working intelligence issues for the first time. The cumulative effect of questions from the field and our own assessment of IOB matters coalesced in a determination that the issuance of comprehensive guidance would be appropriate.

The FBI's response to the recent IG report concerning NSLs demonstrates the willingness of the FBI to accept constructive criticism, incorporate lessons learned, and improve our policies and procedures.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.097

d. The guidance issued by OGC in November 2006 is for field agents to send documents to OGC to determine what to do with them. If there's no overarching policy, how does OGC know what to do with them?

Response:

The November 2006 guidance concerned the reporting of potential IOB violations, not the retention of potentially improperly received information per se. The guidance provides that documents or records that are the subject of a potential IOB violation should be sequestered with the Chief Division Counsel (CDC) pending adjudication of the potential IOB matter. The import of that guidance was not that OGC would retain improperly obtained documents, but that OGC would, as required by Executive Order 12863, make the determination as to whether a potentially improper receipt of documents should be reported to the IOB. OGC has long advised that field offices should *over-report* rather than *under-report* potential IOB matters; that advice is based on the premise that, when there is any doubt as to whether a particular incident constitutes a violation of any requirement under the cognizance of the IOB, it is better to report it than not. Regardless of whether an overproduction of material is reported to the IOB, if the material is not relevant to an authorized investigation, it will be destroyed.

e. If field agents determine documents they received were improperly collected and they send them to OGC, on what possible grounds could OGC decide to retain them?

Response:

Please see the response to subpart d, above.

f. The IG report indicated the information gathered with NSLs is often used to close FBI cases by proving the subject has no links to terrorism. Yet the FBI does not have a policy of purging this data from FBI databases. Why not?

Response:

The FBI has legitimate investigative reasons for retaining information properly collected during the course of authorized investigations, even if the data pertains to individuals who are ultimately determined not relevant to the investigation (for example, the target called a telephone number ten times, but the contact is determined to be innocuous).

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00087 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.098

The FBI retains such information for at least two investigative reasons. First, by retaining the records that form the basis for our determination that a person is not of investigative interest, we ensure ourselves of an audit trail so we do not re-investigate the person each time he or she appears in an investigation. Instead, our agents and analysts can simply revisit the information previously collected and satisfy themselves that the judgment previously made, that this person is not of concern to the FBI, is still valid. That can generally be done without intruding again on the person's privacy and without again collecting personal information about the individual. In contrast, if we were to destroy the data, we would have to re-investigate the person each time he or she became pertinent to an investigation. Accordingly, retaining information is more protective of privacy interests than would be a policy mandating destruction.

The second reason to retain information is equally important: in order to fulfill our mission of keeping the country safe, we have been exhorted by Congress, the 9/11 Commission, the WMD Commission, and the American public to "connect the dots." The reality of analysis and investigative work is that connections between people that may seem entirely innocuous today can seem anything but innocuous when additional information is obtained. For that reason, we need to retain data and analysis regarding individuals so that, should the factual background change, we still have the lawfully obtained information regarding those individuals. In short, using the jargon that has become prevalent, we cannot "connect the dots" if we do not maintain the "dots" to connect.

For these reasons, the FBI does not support a policy that requires the destruction of data merely because, upon initial analysis, the person to whom it relates appears irrelevant to national security concerns.

g. If agents aren't reviewing the material they receive from NSLs, and are uploading that data into FBI databases, how can the FBI be certain its databases aren't bloated with records of totally innocent Americans? Why would the FBI want this information in its databases in the first place? How is it being used?

Response:

We do not read the IG's report as indicating that FBI Agents are not reviewing the material produced pursuant to NSLs. Rather, we believe the IG was concerned that the FBI may not be verifying that the records received were those requested from the provider before uploading them for analysis. This concern was addressed in a January 3, 2007 electronic communication (EC) that reiterated the

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.099

need to review results before uploading to ensure the correct results are being received.

38. With respect to NSLs being used to collect intelligence rather than as investigative tool:

a. The IG report reveals that field agents are not even reviewing data received in response to an NSL, which indicates they are not using the data to pursue investigative leads. What can you do about this?

Response:

Please see the response to Question 37g, above.

b. Under the current system, the FBI can't document how useful NSLs are, because it intentionally does not keep records on how these authorities are used. There were more that 140,000 NSL requests in two years, and the IG confirmed only one conviction for material support for terrorism and 152 "criminal proceedings." Considering the 87% declination rate by the Department of Justice for actual prosecutions, how significant are NSLs?

Response:

Please see the response to Question 35, above.

c. The FBI uses control files to issue NSLs where no authorized investigation exists. Why would the Office of General Counsel allow this, much less suggest it when the law clearly says that the NSLs must be relevant to an *authorized* investigation?

Response:

The premise upon which this question is apparently based is erroneous. While a control file was cited in the issuance of NSLs in a compartmented investigation, these NSLs were relevant to an authorized investigation. It is erroneous, therefore, to conclude that investigative activity was conducted under the auspices of a control file and in the absence of an authorized investigation. The use of a control file under these circumstances may have made auditing difficult, but it was not unlawful. Under the circumstances, the need to protect sensitive intelligence sources and methods fully justified this measure.

Notwithstanding the fact that the use of a control file under the circumstances described above was not unlawful, the FBI has adopted a policy pursuant to which

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.100

NSLs should not be issued under control file numbers and investigative activity should not be conducted based on a control file. The February 23, 2007 EC publishing this policy also reiterates that "NSLs are authorized only when the information sought is relevant to an existing national security investigation."

d. The Communications Analysis Unit is clearly not an investigative unit. Why would it be contracting with telephone companies to receive records, and why would the Office of General Counsel approve such contracts?

Response:

The functioning of the Communications Analysis Unit as an investigative unit or an analytical unit does not affect the propriety of issuing an NSL or receiving information in response to an NSL, provided the data sought is relevant to an authorized investigation.

39. In your testimony before the Senate Judiciary Committee, you testified that "We do not have an enforcement mechanism for national security letters." In response to a subsequent media inquiry by the Associated Press, FBI spokesman John Miller indicated the following about your testimony: "He misspoke. He was operating on the standard that existed before the renewal where the enforcement mechanism was not clearly defined." The article then states, "Miller added that Mueller knows the law was changed, but "it just slipped his mind for that moment."

a. Can you please clarify your testimony for the Committee?

Response:

In the USA PATRIOT Act Improvement and Reauthorization Act (Pub. L. 109-177), Congress enacted 18 U.S.C. § 3511(c) to enable the AG to seek from the United States District Court in an appropriate jurisdiction an order directing the NSL recipient to comply with the NSL request. Any failure to comply with such an order from a district court may be punished by the court as contempt.

b. In addition, can you describe in detail the procedures for the FBI to follow the enforcement mechanism for National Security Letters as established by the reauthorization of the PATRIOT Act in the 109th Congress?

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.101

Response:

Since enactment of the Reauthorization Act, we are unaware of any NSL recipients who have failed to comply with NSLs. When that occurs, the FBI will work with the appropriate DOJ attorneys to enforce the NSL.

40. I am very concerned that Iraqis who have worked with the U.S. government and military are targeted for assassination by terrorists and insurgents. The United States has a moral obligation to assist those whose lives are in danger because of their close association with us. State Department Assistant Secretary Sauerbrey recently testified that Iraqi employees who fear for their lives and already received security checks as part of their employment will nevertheless have to wait six months for the Department of Homeland Security to run an additional security clearance before they are allowed to resettle here.

a. What role does the FBI play in supporting Department of Homeland Security background checks for refugees?

b. What can you do to speed up the clearance process for Iraqis who have a target on their backs because of their association with the U.S. government?

Response:

It is our understanding that DHS does not submit to the FBI name check requests related to background checks for refugees.

41. My constituents frequently write to me with concerns over lengthy times for immigration and naturalization processing. This leaves families separated for months. It also means that thousands of elderly and disabled refugees lose subsistence benefits because they cannot complete naturalization within the seven years for which they are able to receive SSI. I understand that background and other security checks are a big cause of the backlog.

a. What role does the FBI play in this process, especially in the name check process? What are you doing to speed up the FBI's part of the process?

Response:

Through its National Name Check Program (NNCP), the FBI disseminates information from its files in response to requests submitted by Federal agencies, such as the U.S. Citizenship and Immigration Services (USCIS). From the

beginning of FY 2007 through July 31, 2007, the FBI has received over 3.2 million name checks (with over 1.6 million coming from USCIS) and has completed over 3.3 million (with over1.6 million of these belonging to USCIS). Additionally, USCIS submits criminal check requests (the fingerprint portion) to the FBI's CJIS Division for processing.

The FBI is seeking a number of improvements to its process, in the near term, mid-term, and long term.

Near Term

- Working creatively in partnership with other Government agencies to streamline the process. Some agencies have provided employees and/or contractors to assist in the processing of name checks.
- Continuing the development of a computer database that works with the current name check system to eliminate paper processes and the duplicate preparation of reports.
- Completing a new employee development program to streamline the training of new employees in the name check process.
- Scanning all paper files to produce machine-readable documents to build an electronic records system.
- Working with customers to streamline incoming name check requests and automate the flow of information between the FBI and its customer agencies.
- Adjusting the fee schedule to reflect the actual cost of providing name check services. This will provide the FBI with additional resources to address workload demands.

Mid-Term

- Procuring textual analysis software and investigating other ways to further automate the name check process.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.103

Long-Term

- Developing a Central Records Complex to create a central repository of records. Currently, paper files/information must be retrieved from over 265 locations throughout the FBI. The Central Records Complex will address this issue and will create a central document repository and scanning facility.

b. What happens to people who have very common names?

Response:

The processing of common names requires extensive analysis to ensure that any information provided to USCIS pursuant to a name check request is attributed to the correct person.

c. What process exists for expediting completion of the name check process in appropriate cases?

Response:

Name check requests are expedited at the request of the submitting agency.

d. What kinds of changes would you recommend that we make to the current clearance process to allow greater efficiency?

Response:

The FBI is currently implementing several improvements to the Name Check process. Many of these efforts are being undertaken with the USCIS, which is the FBI's largest customer for this service. These improvements, coupled with the additional resources to be provided by the new user fee currently under development, should substantially improve the process.

e. What kinds of changes would you recommend that we make to the current clearance process to allow greater transparency?

Response:

The FBI is committed to working with the USCIS and its other (over 70) customers to provide the information needed for clearance adjudication. The FBI,

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.104

USCIS, and DHS have recently agreed to improvements in the process that will support a reduction in the name check backlog that is consistent with our shared national security and public safety goals.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.105

Questions Posed by Senator Biden

Personnel Issues at the FBI and Their Impact on National Security

1,000 ADDITIONAL FBI AGENTS

42. I noted that in answers to written questions from Senator DeWine you discussed an issue that we discussed privately several years ago - the reprogramming of FBI agents from crime to terrorism. In fact, you indicated that you have lost 994 FBI criminal case agents since September 11th. And, because of this "the FBI has made difficult choices on how to most effectively use the available agents."

My view is that Public safety should be our number one priority, and I think of all the challenges that you are facing with reforming the FBI shortages of agents should not be one. Quite simply, you must have the resources to respond to terrorism AND crime. To this end, I introduced a bill that would authorize an additional 1,000 agents to fill this gap.

Do you view the FBI's responsibility to prevent and respond to crime and would 1,000 additional agents ultimately assist you in meeting the dual challenges of addressing crime and terrorism in the post 9-11 era.

Response:

The FBI's post-September 11, 2001 reallocation of SAs previously assigned to its criminal program did not diminish the FBI's commitment to criminal matters, but it did reduce the number of FBI SAs available to prevent and respond to crime. For a substantial increase in SAs to be fully effective, such an increase should also address the corresponding need for additional equipment and other infrastructure, as well as support employees. If these needs are not addressed, the effectiveness of any additional SAs will not be fully realized.

UP AND OUT POLICY

43. In addition to needing more agents to meet the challenges of crime and counterterrorism, I am concerned that your personnel decisions are compounding the problem. Last year the Bureau began implement a personnel policy related to the Supervisory Special Agents (SSA) wherein SSA with many years of experience supervising investigations are being forced to choose between re-locating to FBI headquarters in Washington or

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.106

accepting a decrease in compensation and giving up their supervisory duties under the so-called "up or out" policy.

Based upon the most recent information, 162 SSA's that were subjected to the "up or out" policy last yea[r], and many of these agents made the decision to leave the bureau rather than [being] re-located to headquarters or give up their supervisory positions. In addition, this year there are roughly 255 SSAs who will be subject to the policy and to this point four have resigned, 15 have stepped down, and 41 have retired.

These SSAs have developed extensive expertise and relationships in their field offices, and I am very concerned that a policy that increases the early retirement of agents with supervisory experience[] harms national security and further exacerbates personnel problems at the FBI.

Are you concerned that losing this many supervisory agents to earlier retirement due to the enforcement of this policy harms counter-terrorism efforts and criminal law efforts within the FBI field offices?

Response:

The Field Office Supervisory Term Limit Policy (FOSTLP) was designed to better position the FBI for the challenges of the future. As the FBI evolves toward a global intelligence-driven agency with increased focus on counterterrorism, hostile intelligence services, and international criminal enterprises, it is important to ensure that our front-line leaders develop a broad base of experience and progress as managers. The FOSTLP promotes the growth and diversification of experience in the supervisory ranks through a strong emphasis on continued career development.

When the FOSTLP was being developed, the FBI considered allowing those SSAs promoted prior to June 2004 to remain in their positions but, given the terrorist threat level and the escalating complexities of criminal conspiracies, the FBI could not afford the luxury of waiting five years before realizing the benefits of this policy. Based on our recognition that those SSAs affected by this policy were among our most experienced mid-level managers, though, a grace period ranging from two to three years based on tenure was established to allow these SSAs an extended opportunity to advance their careers, and several options were made available to accomplish this intent.

Although some of the field SSAs subject to the FOSTLP have relinquished their managerial positions, and some have retired, these results are in line with

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.107

historical data and therefore have not been substantially affected by implementation of the FOSTLP. In addition, many field SSAs have advanced their careers as a result of the FOSTLP rather than returning to investigative duties. For example, the candidate pool for ASACs has increased dramatically since the implementation of the FOSTLP, and field SSAs are filling critical FBIHQ positions such as Unit Chief, Assistant Section Chief, Legal Attaché, and Assistant Inspector. Field SSAs are also participating in other career enhancing opportunities, such as the Alternate Headquarters Credit Plan and the Inspection Team Leader Pilot Project, which are designed to provide experienced field SSAs with the critical FBIHQ experience needed for career advancement.

44. Have you taken any steps to address this problem?

Response:

Please see the response to Question 43, above.

RETENTION OF AGENTS IN HIGH COST CITIES

45. Director Mueller: I am also concerned that the high cost of living is impacting staffing levels and morale of field agents our big cities, where it is imperative we focus our efforts on crime and terrorism. Indeed, assignment of agents to our high-threat cities should be a high priority. I realize that Congress provided pay increases to agents assigned to certain high-cost cities back in 1991.

Is it your view that the parameters of this program are suitable to meet the needs of your work force and to enhance retention in high cost cities?

Response:

The reference to 1991 legislation appears to relate to the New York demonstration project, the authority for which expired many years ago. The FBI does, though, use several other statutory authorities to address the impact of the high cost of living experienced in some of our cities.

The Federal Workforce Flexibility Act of 2004 allows the FBI to offer retention or relocation bonuses in appropriate cases, and the Consolidated Appropriations Act of 2005 (CAA) affords to the FBI specific authority to address the impact of living in high cost areas. The CAA allows the FBI Director to offer bonuses of up to 50 percent to retain FBI employees with unusually high or unique qualifications or to relocate FBI employees to areas with higher costs of living

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.108

than their current residences (as determined by the Director). Although the FBI has used both of these authorities to assist our SA retention efforts, the language of the CAA regarding relocation bonuses is limiting, because it applies only to individuals "transferred to a different geographic area with a higher cost of living." This language does not allow the FBI to offer relocation incentives to those SAs needed in many high cost areas. For example, the CAA does not allow the FBI to offer a relocation bonus to an SA relocating from New York City or Los Angeles to Washington, D.C., because it is not clear that the cost of living in Washington, D.C., is higher than it is in New York City or Los Angeles. In addition, the CAA expires on December 31, 2009, so we cannot build a retention program on which SAs can rely into the future.

46. The use of housing allowances have been used effectively by other agencies, such as the Department of Defense, have you taken any steps towards establishing a housing allowance or other steps to help ensure retention in high-threat, high-cost cities?

Response:

We have considered various means of improving our retention of SAs in high cost areas. A housing allowance would require statutory authority, since the FBI does not currently have the authority to offer housing allowances. We would be pleased to work with OMB, Congress, and others in DOJ to evaluate housing allowances and other incentives to encourage our SAs to relocate to, or remain in, high-threat, high-cost cities.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.109

Questions Posed by Senator Schumer

47. John McKay, the former U.S. attorney in the Western District of Washington, reportedly faced complaints about his decision not to prosecute allegations of election fraud in Washington's 2004 gubernatorial election. Did the FBI agree with Mr. McKay's decision not to prosecute allegations of election fraud in Washington's 2004 gubernatorial election, discussed above?

Response:

Pursuant to a citizen's complaint, the FBI's Seattle Division reviewed allegations of voter fraud in Washington State's 2004 gubernatorial election. The Seattle Division and the U.S. Attorney's Office for the Western District of Washington agreed that the information presented and the substance of the allegations did not merit a Federal investigation. The alleged voter fraud appeared to be individual voter misconduct, which would fall under the jurisdiction of Washington State authorities.

48. David Iglesias, the former U.S. attorney from New Mexico, was also reportedly criticized for his handling of allegations about flawed voter registration cards in the 2004 election. Did the FBI agree with Mr. Iglesias's decision not to prosecute any case about flawed voter registration cards in the 2004 election, described above?

Response:

The FBI's Albuquerque Division agreed with DOJ, including the United States Attorney's Office (USAO) for the District of New Mexico, that there was insufficient evidence to support Federal charges of election fraud in that case.

49. In the judgment of the FBI, was there sufficient evidence to support any federal charge of election fraud in the matters handled by Mr. McKay and Mr. Iglesias?

Response:

The FBI agreed with the decisions of United States Attorneys McKay and Iglesias regarding the election fraud matters at issue.

50. In the judgment of the FBI, were there any election fraud allegations that merited federal charges, but were not pursued, in the jurisdiction of any of the U.S. attorneys asked to resign in 2006?

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.110

Response:

The FBI is not aware of any 2004 election fraud allegations that merited Federal charges but were not pursued in the jurisdictions of the United States Attorneys asked to resign in 2006.

I also ask that you provide the following:

51. Copies of any documents in the custody, control or possession of the FBI regarding the allegations of election fraud in Washington discussed above and the FBI's recommendations in that matter;

52. Copies of any documents in the custody, control or possession of the FBI regarding the allegations of voter registration fraud in New Mexico, described above, and the FBI's recommendations in that matter;

53. Copies of any documents in the custody, control or possession of the FBI regarding allegations of election fraud that were investigated by any other U.S. attorney who was asked to resign in 2006, and the FBI's recommendations in those matters; and

54. Any other documents in the custody, control or possession of the FBI that are relevant to election fraud matters handled by any of the U.S. attorneys who were asked to resign in 2006.

Response to Questions 51 through 54:

These documents were also requested pursuant to a letter from Senator Schumer to Director Mueller dated April 2, 2007 and will be addressed separately.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.111

Questions Posed by Senator Specter

FUNDING FOR NATIONAL SECURITY MATTERS

55. At the hearing, I asked you whether the FBI has sufficient funding for intelligence and counterintelligence matters to protect the nation from another terrorist attack. You replied, "We have requested funds that we have not received, whether it be through the Department of Justice or through the budget process. So there are items we need and would want that would enhance our ability to protect the American public."

a. Please explain what funding the FBI has requested for these priority programs and not received.

b. Also, please respond in writing to my follow-up question at the hearing: "How much additional funding does the FBI need on intelligence and counterintelligence matters to protect the nation from another terrorist attack?"

Response:

The FBI continues to work with OMB and others in DOJ to identify areas of future investment necessary to support both the national security and law enforcement missions of the Bureau.

JUSTICE DEPARTMENT INSPECTOR GENERAL'S REPORT ON NATIONAL SECURITY LETTERS (NSLs)

56. The Inspector General's report on NSLs states that, when the FBI's Office of General Counsel learned of the problems with the "exigent" letters in 2004, it began to implement corrective measures such as "discontinuing the use of exigent letters except in true emergencies." In contrast, reports in the *Washington Post* and the *New York Times*, as well as testimony before the House Judiciary Committee by FBI General Counsel Valerie Caproni, suggest that the FBI was not fully aware of the problem until 2006. Furthermore, the *Washington Post* and the *New York Times* have reported that Bassem Youssef - who currently heads the FBI unit that improperly used the exigent letters - raised concerns about the improper use of exigent letters when he took office in early 2005. The reports say that his concerns were ignored. According to his lawyer, Steve Kohn: "He discovered [the exigent letter procedures] were not in compliance, and then he reported that to his chain of command. They defended the procedures and took no action ... their initial response was to deny the scope of the problem."

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.112

a. When did the FBI's Office of General Counsel first become aware of the problem with so-called "exigent" letters?

Response:

As noted in the response to Question 32, above, multiple reviews of the exigent letter matter are currently underway. It appears that some FBI OGC attorneys may have become aware of aspects of the exigent letter practice sometime in late 2004.

b. When were corrective measures taken?

Response:

Upon learning of the exigent letter practice, and continuing into 2006, OGC attorneys offered a series of recommendations concerning this practice, among which were that exigent letters were inappropriate in the absence of a true emergency. As noted in the response to Question 32, above, multiple reviews of the exigent letter matter are currently underway.

c. Were the concerns of Mr. Youssef ignored?

Response:

As noted in the response to Question 32, above, multiple reviews of the exigent letter matter are currently underway. It should be noted, however, that the IG has testified that SSA Youssef did not raise the exigent letter with the IG when he was interviewed and that Youssef, himself, signed at least one exigent letter.

57. You have said that the FBI plans to remedy many of the problems addressed in the NSL Report. With regard to the misuse of exigent letters, in your written testimony, you said that the General Counsel's office "has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided." You also said that, at last count, "there were still a small handful of telephone numbers that had not been satisfactorily tied to an authorized investigation. If we are unable to determine the investigation to which those telephone numbers relate, they will be removed from our database and destroyed."

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.113

a. Other than removing improperly obtained information from the database, what is the remedy for those people whose privacy was violated by improperly used exigent letters?

Response:

There is no statutory remedy for individuals whose records may have been improperly obtained through the use of exigent letters. That said, it should be noted that telephone information obtained by the FBI pursuant to NSLs is normally received in bulk on computer disks and consists largely of dates, times, and durations of calls. No person's privacy is invaded beyond the bare receipt of this telephone record information unless link analysis or other investigation reveals that the communications are of legitimate investigative interest.

b. Although the IG "did not find any indication that the FBI's misuse of NSL authorities constituted criminal misconduct," will you hold FBI personnel who signed exigent letters accountable if you find they knew there were no exigent circumstances or they knew there was no contemporaneous intention to seek legal process (such as a subpoena)?

Response:

The DOJ IG and the FBI's Inspection Division are conducting a joint investigation into the use of exigent letters. When those inquiries are complete, the Director will determine what steps should be taken.

58. In years past, you have asked this Committee to consider authorizing the FBI to issue administrative subpoenas in counterterrorism cases. Given the lack of internal controls identified in the Inspector General's report on NSLs, why should Congress consider giving the FBI even greater authority to obtain records and other materials unilaterally, without court supervision?

Response:

If we are to be able to protect the United States from terrorist attacks, we must have access to the kinds of information obtainable by NSLs or administrative subpoena. As discussed in response to Question 35, above, the kind of data obtainable by NSL is mission essential, serving as a critical factor in our ability to produce leads that help identify terrorist networks. While NSLs are extraordinarily useful, they do have limitations. Unlike administrative subpoenas, NSLs reach only a narrow type of third-party records. The concerns voiced by

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.114

the IG indicate confusion on the part of some FBI agents regarding the technical requirements imposed by the NSL statutes. The IG did not identify any intentional FBI misuse of its investigative authorities or indication that the FBI was engaging in investigations based solely on the exercise of First Amendment rights or other prohibited criteria. The FBI's response to the IG's concerns shows its willingness to address any perceived gaps in training or errors in the implementation of its lawful authorities.

U.S. ATTORNEY DISMISSALS AND FBI POLICY OF NOT RECORDING INTERVIEWS

59. The FBI has a policy of not recording its interrogations electronically, in contrast to the more than 500 police departments in all 50 states that now make electronic recordings of at least some interrogations. This policy has received publicity in connection with the dismissal of U.S. Attorney Paul Charlton and the trial of I. Lewis "Scooter" Libby. Specifically, a March 4, 2007 *New York Times* story states that Charlton "annoyed Federal Bureau of Investigation officials by pushing for confessions to be tape-recorded." With respect to the Libby trial, a February 12, 2007 *New York Times* op-ed by Adam Liptak observes that jurors in the Libby case had to "rely on an F.B.I. agent's recollection, based on notes," because key interviews were not recorded. The author asks: "Why is the Federal Bureau of Investigation still using Sherlock Holmes methods" in the age of computers?

a. Did the FBI complain about Paul Charlton's efforts to require the recording of interviews?

Response:

In a letter dated February 9, 2006, then United States Attorney Paul Charlton advised Federal law enforcement agencies in the District of Arizona that beginning March 1, 2006, the Arizona USAO would require law enforcement agencies to record, by either audio or audio and video, the statements of all criminal suspects. On March 1, 2006, Charlton advised that he was delaying implementation of this policy while DOJ reviewed it in conjunction with law enforcement agencies to determine whether it should be a pilot project for the broader implementation of this policy. Under the policy, the Arizona USAO would not pursue prosecution if investigative interviews were not recorded, with limited exceptions, even if other evidence supported criminal charges. The policy permitted reasonable exceptions at the sole discretion of the AUSA assigned to the case and that attorney's supervisor.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.115

Because this policy created a requirement not recognized in the Rules of Evidence, and imposed on the government a penalty not applied to other similarly situated parties, the FBI sought DOJ review before implementation. Specifically, the FBI disputed United State Attorney Charlton's claim that the lack of a recorded confession was a key factor in the negative outcomes in three criminal cases, noting that a number of other factors had contributed to those outcomes. The FBI also disputed Charlton's description of FBI policy as prohibiting the recording of interviews or confessions, noting that the FBI's Phoenix Division was already recording many such statements and that other FBI field offices also record subject interviews. Pursuant to the FBI's current policy, which has been in effect since 1998, Special Agents in Charge (SAC) can authorize the recording of confessions and witness interviews in all types of cases, ranging from traditional criminal investigations to national security investigations. The FBI's policy recognizes that many factors are considered when deciding whether to record a confession or interview, and that a blanket requirement mandating recording in all cases would be unnecessarily burdensome. SACs receive substantial guidance regarding the relevant factors and are afforded the discretion to weigh these factors in making their decisions.

b. Do you believe the FBI's policy complicated the Libby prosecution?

Response:

As indicated in response to subpart a, above, the FBI's policy does not preclude the electronic recording of interviews. Instead, this decision is made on a case-by-case basis, and the determination not to record the interviews in this case was made because it was believed that doing so would chill the fact-gathering process, hampering the investigation rather than forwarding it. In this case, in particular, the absence of recordings had no adverse impact on the Libby prosecution because Libby and other critical witnesses were examined during the grand jury process, so a word-for-word transcript of their testimony was created at that time.

c. Why does the FBI maintain this policy?

Response:

The FBI's practice of recording some, but not all, interviews is consistent with the practice of many other law enforcement agencies. While the policies of law enforcement agencies vary widely in this regard, they rarely mandate the recording of all interviews. The FBI's policy of permitting the SAC to authorize recording as required by investigative needs recognizes that local policies vary

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.116

and that recording does have some investigative and practical disadvantages. For example, a requirement to record all interviews would be quite expensive, would create significant logistical challenges, and may create obstacles to the admissibility of lawfully obtained statements that are not recorded through either inadvertence or circumstances beyond the control of the interviewing agents. In addition, the very presence of recording equipment may actually undermine the FBI's highly successful rapport-building interview technique.

Additional information responsive to this request is provided separately.

INTELLIGENCE ANALYSTS

60. At a January 2007 Intelligence Committee hearing, Deputy Director John Pistole said the FBI has hired roughly 2200 intelligence analysts. At the same hearing, Dr. John Gannon stated that FBI analysts are "given minimal training and deployed into organizations that are managed by agents." He then compared this unfavorably to how analysts are treated in the CIA and DIA.

a. Please describe the general experience and background of the analysts hired by the FBI.

Response:

In the past 3 years, the FBI has been successful in recruiting and hiring 1,488 Intelligence Analysts (IA) with the skills and backgrounds needed to build the FBI's intelligence program, including those with general analytic skills, those with particular specialized skills, and those with the specific knowledge needed to understand and analyze particular types of information. The FBI's IAs come to us from various positions and backgrounds, including other Intelligence Community (IC) agencies, academia, state and local law enforcement, the United States military, and the private sector, and have a wide range of critical skills in such subject areas as regional studies, international security, law, computer engineering, computer science, engineering, financial security, international banking, international migration, Islamic studies, physical science, religious conflict, and weapons of mass destruction (WMD).

This successful recruitment effort was conducted pursuant to a targeted recruitment strategy that identifies the critical skills the FBI needs to satisfy its current responsibilities as well as those required to address its future needs. The FBI is updating its IA recruitment strategy to reflect the current hiring

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.117

environment within the intelligence workforce and anticipates releasing a modified version of this strategy by the end of 2007.

b. What training are they provided by the FBI?

Response:

The FBI's intelligence training is designed to align with IC standards for content and tradecraft, addressing the policy, authorities, and oversight requirements relevant to a robust domestic intelligence mission, augmented as appropriate by material uniquely relevant to the FBI's dual missions of intelligence and law enforcement. To ensure that training remains a top FBI priority, the FBI's Directorate of Intelligence (DI) has established a special assistant position specifically focused on training. Below are descriptions of the courses and training initiatives designed to meet the needs of the FBI's IAs.

Intelligence Analyst Courses

- Intelligence Basics Course (IBC) – In collaboration with the FBI's Training Division (TD), the DI is currently redesigning the entry level course for new analysts. This course will emphasize the three tradecraft skills (thinking, expository writing, and briefing) critical to an analyst's professional success and necessary to the production of more sophisticated, forward-leaning analysis and to its effective delivery to a range of consumers. The IBC will give students a solid foundation for their continued professional development by exposing them to a variety of techniques and exercises that will improve their ability to: think creatively but check the insights they develop with rigorous, structured, and skeptical scrutiny; craft accurate, concise, and comprehensible written products for consumers who have very little time to read and understand them; and deliver the same high quality analysis orally under a variety of circumstances. Students who finish the IBC will be better prepared to fulfill a variety of roles at the FBI and to contribute to the success of its unique intelligence mission. This 10-week course will be comprised of modules that can be used in various combinations to provide tailored training to a field office or to groups of field offices.

- Managing Analysis Course - In coordination with the TD, the DI has conducted the Managing Analysis Course, which was piloted in August 2006, on two additional occasions. This course was developed to enhance the effectiveness of those responsible for supervising analysts; many

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.118

supervisors are not, themselves, analysts. The workshop, which will be presented over days using a variety of exercises, provides supervisors with a set of tools and management techniques they can use to enhance the rigor and quality of the analytic products generated by their offices. The workshop addresses such issues as the role of analysis in the intelligence cycle, categorizing various types of analysis, how to avoid analytic traps and mind sets, selecting and characterizing evidence, meeting the needs of various customers, elements of effective warning, and understanding analysts and their core competencies. The last half day will be taught by DI personnel and will include discussions of the intelligence production and review process and of the promotion process. Feedback regarding this course, which requires both pre-workshop and evening homework, continues to be positive, and we are making adjustments to optimize the value of the course. To date, 115 students have received this training.

- Reports Officer Course - In coordination with the TD, the DI ran a pilot of the newly developed one week basic Reports Officer (RO) course in January 2007. This course was designed to give entry-level ROs a clear idea of their responsibilities and to enable them to achieve greater consistency in their duty performance. Participants will learn about RO roles and responsibilities, the national requirements structure and collection requirements process, what intelligence is and how to discern intelligence information from operational information, the importance of Intelligence Information Report (IIR) follow-up, and the legal authorities that govern collection and reporting. The course will teach students how to refine techniques for drafting various intelligence products, including division-specific IIRs, teletype memos, requests for information, and responses to *ad hoc* requirements. Additionally, participants will benefit from a panel discussion with experienced ROs and be challenged by an intensive IIR practical writing exercise. Feedback from the pilot course has been very positive and we are in the process of making appropriate changes suggested by developers, instructors, and the pilot's students.

- Collection Management Course - This course provides overviews of intelligence collection requirements management, collection operations management, and the national intelligence prioritization and needs process, and provides familiarization with open source intelligence, the Open Source Requirements Management System, imagery intelligence, signals intelligence, measurement and signature intelligence, and human intelligence. The course will be taught at Quantico by a mobile training

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.119

team from the Defense Intelligence Agency (DIA) Joint Military Intelligence Training Center (JMITC).

- Counterdrug Intelligence Analyst Course - This course will examine the nature of organized criminal activity in drug trafficking and serves as a baseline for understanding the techniques, tools, and procedures used to analyze these organizations and derive intelligence. It will be taught at Quantico by a mobile training team from DIA's JMITC. Additional iterations will be offered based on demand.

- Counterintelligence Analytic Methods Course - This course provides a counterintelligence foundation for IAs who work strategic and operational-level all-source analytic issues. The analyst will also be able to demonstrate a counterintelligence methodology that accurately evaluates assets, threats, vulnerabilities, and risks associated with FBI counterintelligence support activities. The counterintelligence analyst's relationships with collectors and customers are continually examined and emphasized during the four day course. This course will be taught at Quantico by a mobile training team from DIA's JMITC. Additional iterations will be offered based on demand.

- Counterterrorism Analyst Course - This course introduces new counterterrorism analysts to the nature and extent of the terrorism threat and associated analytical challenges and techniques. Emphasis is placed on student collaboration and multiple exercises. This course will be taught at Quantico by a mobile training team from DIA's JMITC.

- WMD Terrorism Course - This workshop provides a basic overview of the technical and terrorist threat aspects of nuclear, chemical, and biological weapons. Participants will be introduced to counterterrorism policy and to the various Federal Response Elements and the role each plays when responding to a WMD event.

- Financial Intelligence Seminar (DIA) - This seminar provides analysts with the basic tools needed to uncover the trails of money that support terrorist activity, are generated by narcotics cartels, or result from other international crimes. The goals of the course are to apply financial analysis techniques, in the context of critical thinking and structured analytic techniques, to improve the quality of financial analyses and assessments of intelligence target operations. The seminar provides tools and techniques for analyzing financial networks and developing actionable

---

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.120

intelligence. It focuses on how money moves through banks, money services businesses, and informal value transfer systems (such as hawalas), examining the impact this movement has on operational decisions. The seminar includes learning blocks on money laundering schemes and indicators, terrorism financing, financial critical thinking, and trade-based transfer systems. In the financial analysis section, the students will study sources of information, bank record analysis, financial patterns, financial data charting, and financial profiles. The course is capped by a three and a half hour interactive exercise involving multiple bank accounts. Financial experience or background is not a prerequisite for taking the course.

Domain Management

- Fundamentals of Geographic Information Systems – As part of DI's effort to implement domain management practices and methodology, the DI has, in partnership with the National Geospatial-Intelligence Agency, tailored a one week course that teaches basic applications of geographic information systems in FBI domain management. During FY 2007, DI will host seven such classes. These classes have been attended by both FBIHQ and field SAs and IAs.

Tools and Techniques

Analyst Notebook - The Analyst Notebook training will be presented over four and a half days using a variety of exercises. Students will learn the fundamental concepts and features necessary to create and analyze Association and Timeline charts. Using scenario-driven exercises, students will learn how to: manually create charts and import structured data to make charts; use basic functional tools with the software to query, find, and analyze data within the charts; switch a chart from association to temporal or vice versa; merge and combine charts; use attributes in charts; and set up charts for presentation.

Pen-Link - The three day Pen-Link course provides instruction regarding various Pen-Link databases, including Calls, Subscribers, Events, Seizures, Case Management, City-Link, and International, as well as multi-media storage and Title III (wiretap) information. Students will become familiar with basic configuration options, manual data entry, Pen-Tran, built-in database reports, built-in frequency reports, built-in special reports, graphic analysis, and custom reporting.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.121

Denial and Deception - This course discusses methods used by foreign governments and groups to deflect and distort intelligence collection and analysis. The course, which will be taught at Quantico by a mobile training team of DIA's JMITC, will provide an introduction to the methods and tools available for identifying and neutralizing foreign denial and deception tactics. Additional iterations will be offered based on demand.

Open Source Intelligence Course (Hidden Universes) - This three day course, which will be taught by Open Source Academy instructors, will offer a baseline understanding of the rich, complex, and dynamic world of open-source information as leveraged by the IC. The course will also introduce the latest tools and strategies that help IC personnel exploit open sources quickly, efficiently, and knowledgeably, and will familiarize students with the basic elements of a robust open source acquisition, exploitation, and dissemination process.

Advanced Tools and Techniques - This course engages analysts in a highly interactive, hands-on environment and covers some 20 tools and techniques that can enhance the sophistication and rigor of finished analytic products. Analysts participate in numerous practical exercises using tools such as argument mapping, brainstorming, key assumptions check, red cell analysis, analysis of competing hypotheses, social network analysis, advanced devil's advocacy, risk security analysis, and others. In addition, students will engage in interactive discussions of analytic traps and mind-sets, how to collaborate more effectively in virtual environments, how best to use these tools and techniques in written products, and how to integrate these advanced tools and techniques into their daily work process.

c. How does the training provided to analysts by the FBI, in terms of curriculum, duration, and similar factors, compare to the training provided by the CIA and DIA?

Response:

The FBI is orienting its training for new analysts to mirror the CIA's new analyst training. After reviewing other organizations' courses for new analysts, including those run by the CIA, DIA, and NSA, the FBI determined that the CIA's Career Analyst Program (CAP) was most closely aligned with the FBI's intelligence

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.122

requirements. In revising our basic intelligence training for new analysts and developing the new IBC, we have been using the CAP as a template.

The FBI's 10-week IBC is designed to introduce our new analysts to the world of intelligence and analysis while focusing on three fundamental skills: critical thinking, expository writing, and briefing. We have developed a close working relationship with the CIA's Kent School and are adapting a number of the CIA's core modules and exercises for use in the IBC.

Immediately following the restructuring of the IBC curriculum, the FBI will begin adapting key modules for delivery to FBI employees who supervise analysts. We anticipate a three to five week "Developing Analysts" course that will help ensure that analysts and supervisors, regardless of position, have the same vocabulary and are on the same analytic page conceptually.

d. To what extent has the Director of National Intelligence implemented standardized training for analysts in the Intelligence Community?

Response:

- While the Office of the Director of National Intelligence (ODNI) has not required that the FBI conform its training to an ODNI standard, it has offered guidance through the provision of training competencies, the Intelligence Community Officer Certification Program, ODNI-sponsored training and programs, and presentations by various leadership speakers. Below are some examples of ODNI-sponsored initiatives in which the FBI is actively engaged.

Intelligence Community Training Initiatives

- Intelligence Community Officer Training (ICOT) - The ODNI-sponsored ICOT certification requires 400 hours of training in the following seven categories: National Security and Intelligence Issues; Leadership and Management; Counter Intelligence (CI), Security, Information Assurance, Denial and Deception; Production and Analysis of Intelligence; Collection, Sources, and Processing of Intelligence; Impact of Intelligence across the IC; and the IC Officer Course. While training may be obtained from a variety of sources, including IC classes, the FBI, or universities, course objectives must relate to at least one of the aforementioned categories to receive credit for ICOT certification purposes. To date, one FBI IA has earned IC Officer certification.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00112 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.123

Intelligence Community Assignment Program (ICAP) – ICAP, a structured rotational program within the IC, is designed to provide intelligence professionals (GS-13s, 14s, and 15s, as well as highly qualified GS-12s) with the opportunity to gain IC experience through rotational assignments in intelligence or intelligence-related positions associated with the participants' parent organizations. Two FBI employees have completed ICAP tours and are eligible for ICAP certification pending completion of end-of-tour surveys. Two more candidates are expected to complete ICAP tours next year and would then be eligible for ICAP certification in 2008.

Summer Hard Problem Program (SHARP) – SHARP is a four week program sponsored by the Office of the Deputy Director of National Intelligence for Analysis. Students in this program investigate the intelligence implications of the factors that cause individuals and communities of interest to coalesce into pro-social, antisocial, terrorist, or extra-legal movements. FBI participation in the 2006 initial offering was praised, and the FBI has been encouraged to nominate candidates for upcoming programs.

Rapid Analytic Support and Expeditionary Response (RASER) Team - Four FBI IAs joined other IC colleagues in the two year ODNI-sponsored RASER program. The purpose of the RASER team is to establish a group of multidiscipline, highly-trained analysts ready to deploy worldwide on demand. ODNI tasked each of the IC agencies to nominate five candidates for the 12 positions; all five of the FBI's applicants were awarded positions on the team.

ODNI Leadership Day Speakers Series - The FBI hosted ODNI's first annual Intelligence Community Leadership Day. Presenters from the FBI included the FBI's senior leadership, as well as leaders from across the IC. The FBI will continue to participate in this series and plans to send approximately 30 senior-level employees to the next ODNI Leadership Day.

TERRORIST IDENTITIES DATAMART ENVIRONMENT (TIDE) AND THE TERRORIST SCREENING CENTER (TSC)

61. The *Washington Post* has reported that, each day, thousands of pieces of intelligence information from around the world are fed into a central list of terrorists and terrorism suspects known as TIDE, which is maintained by the National Counterterrorism Center.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00113 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.124

According to the *Post*, TIDE has "[b]alloon[ed] from fewer than 100,000 files in 2003 to about 435,000." Moreover, "the growing database threatens to overwhelm the people who manage it." According to the article, "The bar for inclusion is low, and once someone is on the list, it is virtually impossible to get off it. At any stage, the process can lead to 'horror stories' of mixed-up names and unconfirmed information." The article even quotes Russ Travers, the official in charge of TIDE, as saying: "The single biggest worry that I have is long-term quality control."

The article adds, "Every night at 10, TIDE dumps an unclassified version of that day's harvest -- names, dates of birth, countries of origin and passport information -- into a database belonging to the FBI's Terrorist Screening Center." The article acknowledges that, for inclusion in the FBI's database, the "bar is higher than TIDE's," leading to total listings of about 235,000. Nevertheless, the article raises several issues:

a. Do you have concerns that these lists are growing too large to manage?

Response:

The FBI pursues a counterterrorism watchlist strategy designed to enable law enforcement and screening personnel to effectively detect, disrupt, and/or track those suspected of participating in terrorist networks, requiring that the subjects of both preliminary and full-field investigations be watchlisted. The FBI's TSC continues to monitor the growth of the Terrorist Screening Database (TSDB) to ensure that its collection strategy is appropriate, that it is maintained consistent with the policy set forth in Homeland Security Presidential Directive 6, and that it serves the needs of its customer agencies. In collaboration with these customer agencies, TSC continues to examine the data collection methodology to ensure the terrorism screening process is as efficient and effective as possible.

b. Given the problems with internal controls elsewhere at the FBI, are you confident that these systems are not infringing on the privacy rights of innocent people?

Response:

The TSC has a robust privacy compliance program in place, led by a full-time Privacy Officer, to ensure the personal information TSC maintains is protected by strong privacy and security policies and practices. The TSC Privacy Officer reports to the TSC Director and is responsible for establishing internal policies and procedures to ensure the TSC complies with the laws and policies regulating the handling of personal information and to recommend additional policies that would enhance compliance with information privacy principles.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00114 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.125

Following are examples of the TSC's efforts to ensure privacy rights are protected.

- The TSC has implemented quality controls at the various stages of the watchlist process to increase the quality of TSDB data. For example, in March 2006, TSC began to use a newly developed business process (known as the Single Review Queue) to ensure every new nomination or modification of a watchlist record is reviewed for quality by a member of TSC's Nominations Unit before inclusion in the TSDB. TSC analysts review the nominations to ensure, to the extent possible, the accuracy of biographical data and the sufficiency of the derogatory information supporting the watchlist nomination. Nominations are refused if they are not supported by adequate biographical information or derogatory information indicating a nexus to terrorism.

- The TSC's redress process provides for timely and fair review of individuals' complaints and the correction any data errors, including errors in the terrorist watchlist itself.

- The TSC's Data Integrity Unit is continually reviewing TSDB data to ensure it is accurate, thorough, and current. Examples of efforts by the Data Integrity Unit are the recently completed 100 percent review of the No Fly List and the ongoing 100 percent review of the Selectee List.

- The TSC has developed procedures to ensure that, every time a possible encounter with a watchlisted person is phoned into the TSC, an Operations Specialist assigned to the Terrorist Screening Tactical Operations Center reviews the relevant entries in the TSDB and other relevant data systems for completeness and accuracy. If a record is determined to be accurate and complete, it is maintained. If, however, modification or removal appear to be necessary, the TSC coordinates with the nominating agency and the National Counterterrorism Center to ensure the record is adjusted or removed, as appropriate.

- The TSC has performed privacy impact assessments of its information technology systems in compliance with the e-Government Act of 2002 and has published a Privacy Act notice describing its system of records in compliance with the Privacy Act of 1974.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00115 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.126

- The TSC has integrated privacy risk assessments into various parts of the information technology system development life cycle to ensure privacy risks are identified early and mitigated appropriately.

- The TSC has developed and applied to the TSDB technology-oriented business rules designed to identify records that appear to have erroneous, inconsistent, or otherwise discordant data and to ensure prompt correction of this information.

- The TSC is reviewing staffing needs to ensure the availability of adequate staff to conduct audits and internal compliance reviews to improve both data quality and the efficiency of business processes.

DOMESTIC SPYING BY THE NEW YORK POLICE DEPARTMENT

62. The *New York Times* has recently reported that the New York Police Department (NYPD), in preparation for the 2004 GOP Convention, gathered and disseminated intelligence information on what appeared to be lawful political activity: "In hundreds of reports stamped 'N.Y.P.D. Secret,' the Intelligence Division chronicled the views and plans of people who had no apparent intention of breaking the law ... These included members of street theater companies, church groups and antiwar organizations, as well as environmentalists and people opposed to the death penalty, globalization and other government policies."

I understand that an April 2006 Inspector General report titled "Review of the FBI's Investigative Activities Concerning Potential Protesters at the 2004 Democratic and Republican National Political Conventions" cleared the FBI of similar allegations. Nevertheless, the recent reports about the NYPD raise new questions:

a. Did the FBI collaborate with, or give guidance to, the NYPD with respect to intelligence gathering prior to the GOP Convention?

Response:

Along with the Secret Service and the New York Police Department (NYPD), the FBI served on a committee focused on the responsibilities and mechanics of intelligence dissemination during the Republican National Convention (RNC). The committee did not provide guidance regarding intelligence gathering. Instead, the committee focused its efforts on the dissemination of intelligence related to the existing international terrorism threat through the Joint Terrorism Task Forces (JTTFs), in large part based on the fall 2004 threat concern.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00116 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.127

In response to a request from Congress, DOJ's OIG reviewed the FBI's investigative activities with respect to potential protestors at the 2004 Democratic and Republican national political conventions. The OIG conducted over two dozen interviews of FBI personnel, including those assigned both to field offices (including New York) and to FBIHQ (including the Counterterrorism Division, Counterintelligence Division, and OGC). The OIG also examined approximately 10,000 pages of documents produced by the FBI in response to the OIG's document requests. Among the documents analyzed by the OIG were FBI investigative case files, information retrieved from FBI databases, correspondence, guidance memoranda, and manuals. The OIG concluded that the FBI's investigative activities were based on the threat of criminal activity and that its investigative conduct was consistent with the applicable Attorney General Guidelines.

b. Did the FBI receive any intelligence information on lawful political activity from the NYPD?

Response:

The FBI's New York Field Intelligence Group (FIG) had SAs and Task Force members embedded in the NYPD Intelligence Fusion Center and elsewhere during the RNC. During this event, the NYPD prepared and disseminated to both the FIG and the FBI's Joint Operations Center (JOC) daily situation reports concerning RNC activities, including arrests, demonstrations, and delegate and VIP movement. The situation reports provided information regarding both legal and illegal demonstrations focusing on location, direction of movement, time, arrests, and participant numbers. The FIG and JOC received real-time intelligence from the NYPD concerning information included in the daily situation reports, and FIG members participated in the formal daily briefings to law enforcement agencies. The FIG assessed this and other information and provided to appropriate customers intelligence related to potential international and domestic terrorism threats both to the United States generally and to New York City and the RNC specifically. This information was included in the NYPD situation reports, which were intended to provide situational awareness for all law enforcement agencies involved with the RNC and were provided to multiple law enforcement agencies. The FIG received the NYPD situation reports and disseminated them internally to JTTFs and FBI personnel involved with the RNC.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00117 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.128

c. In your view, does the fact that the NYPD felt a need to engage in such far-reaching intelligence gathering reflect a lack of confidence in the FBI's ability to provide local law enforcement with necessary information?

Response:

The FBI's mission during National Security Special Events is to support local law enforcement efforts to identify terrorism threats, and it works closely with the JTTFs, which include local law enforcement representatives, to do so. The FBI highly values the contributions of the NYPD and other State and local law enforcement agencies to the JTTF and to other task forces, and strongly believes the JTTF partnership is the most effective way to prevent terrorist attacks.

The relationship between the FBI and NYPD has continued to grow and evolve. The FBI and NYPD have worked together closely to prevent attacks, and both have adjusted operations to address the threat in a manner consistent with their respective authorities. In his September 12, 2006, prepared statement to the Senate Committee on Homeland Security and Governmental Affairs, the NYPD Deputy Commissioner for Counterterrorism, Richard A. Falkenrath, stated: "[T]he NYPD's most important federal partner in the field of counterterrorism [is] the Federal Bureau of Investigation. The NYPD has an excellent partnership with the FBI's field office in New York. . . . [O]ver 100 NYPD detectives are assigned full-time to the Joint Terrorism Task Force in New York City. The JTTF permits the awesome power of the federal government's national intelligence capabilities to be brought to bear against any particular terrorism case. . . ."

LEAK INVESTIGATIONS

63. There was a leak three weeks before the last election about an investigation into Congressman Curt Weldon, who represented Delaware County in the Philadelphia suburbs. The following week, there was a search and seizure at the property of Congressman Weldon's daughter. At your December 2006 hearing, you stated that you were conducting an ongoing investigation of this leak. Can you provide an update on the status of this investigation?

Response:

The FBI has interviewed 121 personnel, 85 of them FBI, as well as a number of other individuals, and analyzed internal records in furtherance of this investigation. The investigators were unable to identify a suspect or substantially

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00118 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.129

narrow the pool of possible suspects. Accordingly, the investigation was closed on October 1, 2007.

These responses are current as of 7/31/07

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00119 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.130

Questions Posed by Senator Grassley

MICHAEL GERMAN TRANSCRIPT

64. through 83.

As Congress has previously been advised, the contents of the transcript are highly sensitive because a person with knowledge of these circumstances could identify the parties from the context provided. Similarly, many of the questions based on the transcript provide sufficient details to permit this identification. The transcript excerpts, the questions, and the FBI's responses are, consequently, provided separately.

JANE TURNER VERDICT

84. Former FBI agent Jane Turner recently won a $565,000 verdict from a federal jury in Minnesota. The jury found that her supervisors had made false and misleading statements in her performance reviews in retaliation for her for filing an Equal Employment Opportunity claim. I recently wrote asking what steps the FBI is going to take to discipline the supervisors responsible for the retaliation. However, all I got back was a letter saying that you don't comment on personnel matters.

a. You say you won't tolerate retaliation, but what are you doing about this? A jury found that FBI supervisors retaliated against someone, why can't you at least tell us whether the FBI is taking any action to consider holding accountable the people who did it?

Response:

The jury found that two of Jane Turner's former supervisors in Minneapolis retaliated against her for her complaints of discrimination. One of them, former Supervisory Senior Resident Agent (SSRA) Craig R. Welken, retired from the FBI in 2001 and the other, former ASAC James H. Burrus, Jr., retired on May 1, 2007.

Some media accounts have incorrectly identified James Casey as one of the FBI supervisors who retaliated against Ms. Turner. Mr. Casey was not assigned to the Minneapolis Division and his only involvement arose from his participation in the October 1999 inspection of the Minneapolis Division, which included the Minot Resident Agency (RA), Ms. Turner's office of assignment. That inspection resulted in Ms. Turner's "loss of effectiveness" transfer from the Minot RA back

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00120 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.131

to the Minneapolis headquarters office, which the jury specifically found did not constitute retaliation.

b. I understand the FBI may appeal the decision. Why is that a wise use of FBI resources? Do you think the jury got it wrong? If so, why?

Response:

After careful consideration by the FBI and DOJ, the judgment was not appealed. In light of the jury's verdict, DOJ determined that an appeal was not in the best interests of the United States.

DeVECCHIO CASE

85. As you know, I've previously expressed my concerns about the appearance given by current and former FBI agents who are publicly supporting Lindley Devecchio. He is a former agent currently charged with four counts of murder in New York, under circumstances similar to the scandals exposed a few years ago in the Boston FBI office. You have assured me that the FBI takes no position and that you will let the legal process play-out in court. However, recently I learned that the Justice Department is paying at least part of Devecchio's legal bills and that the prosecutor's requested documents that the FBI has not provided. For example, the prosecutors in New York would like to see the entire informant file for the mob informant that Devecchio allegedly helped in a mafia war in the 1980's.

a. In order to approve paying his legal bills, did the FBI make any determination or certification that Devecchio acted lawfully and within the scope of his employment?

Response:

Pursuant to regulations governing the representation of Federal employees by DOJ attorneys or by private counsel furnished by DOJ (28 C.F.R. § 50.15), the FBI submitted to DOJ a statement containing its findings as to whether DeVecchio was acting within the scope of his employment and whether such representation would be in the best interest of the United States. This statement was accompanied by all relevant information available to the FBI. All material prepared by FBI and DOJ personnel in this regard is protected by the attorney-client and attorney work-product privileges.

b. Why is the FBI withholding evidence from local prosecutors in a murder trial?

Response:

The FBI is not withholding evidence from the prosecution. Pursuant to applicable Federal law (see, for example, *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951), and 28 C.F.R. § 16.21, *et seq.*), the numerous requests of the Kings County District Attorney (DA) for FBI and other Federal records and information in this case have been handled by the USAO for the Eastern District of New York. The USAO reviewed related FBI records and information in order to properly respond to the DA's requests, proffering the testimony of FBI personnel having first-hand factual information and authorizing the release to the DA of thousands of pages of FBI records. These records included all relevant portions of the informant file of Gregory Scarpa, Sr., the informant with whom DeVecchio is accused of having conspired, and records of all FBI payments made to Scarpa during the relevant time period. To the extent that any related FBI records or information were not produced, this was based upon the USAO's determination that such information was not relevant and that production should therefore not be authorized pursuant to the *Touhy* regulations set forth at 28 C.F.R. § 16.22(d). It is the FBI's understanding that the production of FBI records and information was acceptable to the DA's lead prosecutor, and that the DA's office has made no requests for additional FBI information since August 2006.

c. I understand that the FBI's General Counsel, Val[e]rie Caproni, had some involvement in the underlying facts when she was at the U.S. Attorney's Office in New York. What role, if any, has she played in the decision to withhold documents from the local prosecutors?

Response:

General Counsel (GC) Caproni has played no decision-making role regarding the DA's requests for production of FBI records and information. Pursuant to applicable Federal law, and as discussed further in response to subpart b, above, such decisions have been made by the responsible USAO.

d. Have you analyzed whether it might be appropriate for her to recuse herself from any such decisions?

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00122 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.133

Response:

GC Caproni recused herself from decision-making in this case in April 2006. As discussed in response to subparts b and c, above, decisions regarding disclosures to the DA of FBI and other Federal records and information in this case have been made by the responsible USAO pursuant to applicable Federal regulations.

AMERITHRAX

86. I recently learned from depositions in the lawsuit that Stephen Hatfill filed against the FBI, that you denied the lead investigator's request to polygraph FBI agents. He said he wanted to do that in order to get to the bottom of who in the FBI was leaking information about the case to the press. I also learned that instead, you ordered the three squads working on the case not to talk to each other - to put up stovepipes to prevent sharing information.

a. Why wouldn't you allow the investigators to do what they felt was necessary to find out who at the FBI was leaking?

Response:

The FBI Director has a clear policy against the leaking of confidential law enforcement information, and his communications with those involved in the anthrax investigation were consistent with this policy. As indicated in the Director's deposition, he generally believes that the use of polygraph examinations is productive in investigations involving a narrow universe of individuals to be examined. That was not the case regarding the anthrax investigation leaks, where the universe of possible leak sources included the FBI, DOJ, the U.S. Postal Service, Congress, and others. More central to this particular case, though, is that the leak investigation was handled by DOJ's OPR, not by the anthrax investigation team. In fact, we presume DOJ's OPR would have objected to outside activities that might impact their investigation.

b. Did the FBI take any other steps to find out who was responsible? For example, were the telephone records of agents with access to the information examined to find out if they had been talking to the reporters who published sensitive information? If not, why not?

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.134

Response:

The FBI cooperated fully with the investigation by DOJ's OPR. We defer to DOJ's OPR with respect to the acquisition of telephone records and other investigative steps.

c. Rick Lambert, the former lead investigator, testified that putting up walls between the investigators working different aspects of the case risked keeping the FBI from "connecting the dots" like before 9/11. Given his strong concerns, why did you overrule him and direct that he "compartmentalize" the case?

Response:

It is critical that investigators have access to all relevant information when they are seeking to identify relationships among various facts. Particularly since the attacks of September 11, 2001, the FBI has placed great emphasis on information sharing, and has instituted numerous mechanisms to ensure that we "share by rule and withhold by exception." One "exception" (meaning, one circumstance in which information sharing is not appropriate) is when such sharing would not benefit the investigation at issue, such sharing may adversely affect that investigation (such as by encouraging or contributing to information leaks), and the absence of such sharing is not likely to adversely affect other investigations. This was such a case.

87. Also in the deposition transcripts in the Hatfill lawsuit, there is an indication that the FBI did some kind of background records check on constituents who wrote to their member of Congress about the case and whose letter had been referred to the FBI for comment by the Member of Congress.

a. Does the FBI routinely do these records checks on citizens who contact their elected representatives to inquire about an FBI matter?

Response:

According to the referenced transcript, the deposition witness indicates that when we receive constituent and similar inquiries the FBI queries "ACS." Although the witness indicates that ACS is "the system that the FBI employs and generates peoples' criminal background history," this is not the case. The FBI's Automated Case Support (ACS) system contains FBI-generated documents, including investigative information and other FBI documents uploaded pursuant to FBI policy. While ACS is queried by those familiar with its contents and uses to

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00124 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.135

address the substance of an inquiry (typically by obtaining either substantive case information or the identity of a subject-matter expert who can assist in responding to the inquiry), FBI practice is not to use ACS to obtain information regarding the person making the inquiry, such as a constituent.

b. Were records checks performed on all constituent mail referred to the FBI, or only on those involving the Amerithrax investigation? Were records checks performed only on authors of letters critical of the FBI or supportive of Stephen Hatfill?

Response:

ACS queries are conducted for the purpose of obtaining substantive information to respond to constituent inquiries, not to obtain information about the constituents themselves. This is the case regardless of whether the inquiry concerns the anthrax investigation.

c. Are Members of Congress given any notice that referring a constituent letter to the FBI may result in an FBI records check on their constituent?

Response:

Referring a constituent letter to the FBI does not result in an FBI records check on the constituent.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00125 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.136

SUBMISSIONS FOR THE RECORD

June 26, 2006

Mr. Gregory E. Scarbro
Unit Chief
Federal Bureau of Investigations
Criminal Justice Information Services Division (CJIS)
Module E-3
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

By FAX Machine (304) 625-3566

Re: Comments Solicited under 71 FR 24869
Comments Regarding Hate Crime Statistics Act Report

Dear Mr. Scarbro:

On behalf of the broad coalition of civil rights, education, religious, professional, and civic organizations listed below, we are writing in response to the Department of Justice's April 27, 2006 request for comments on the existing Hate Crime Incident Report form and Quarterly Hate Crime Report form. We believe the FBI has done very fine work in implementing the Hate Crime Statistics Act (HCSA) of 1990, 28 U.S.C. Section 534 Note. We are committed to continuing to work with the Bureau to improve reporting and expand participation in the HCSA data collection initiative.

Background: The Impact of Hate Violence

All Americans have a stake in effective response to violent bigotry. These crimes demand priority attention because of their special impact. Bias crimes are designed to intimidate the victim and members of the victim's community, leaving them feeling isolated, vulnerable, and unprotected by the law. Failure to address this unique type of crime could cause an isolated incident to explode into widespread community tension. The damage done by hate crimes, therefore, cannot be measured solely in terms of physical injury or dollars and cents. By making members of minority communities fearful, angry, and suspicious of other groups – and of the power structure that is supposed to protect them – these incidents can damage the fabric of our society and fragment communities.

The urgent national need for both tough law enforcement response and education and programming to confront violent bigotry has only increased since the September 11, 2001 terrorist incidents. In the immediate aftermath of the September 11 terrorist attacks, the nation witnessed a disturbing increase in attacks against American citizens and others who appeared to be of Muslim, Middle Eastern, and South Asian descent. Perhaps acting out of anger towards the terrorists involved in the attacks, the perpetrators of these crimes irrationally lashed out at innocent people because of their personal characteristics – their race, religion, or ethnicity. In an effective and coordinated response to these backlash hate crimes, law enforcement officials investigated hundreds of such incidents reported from coast to coast – at places of worship, neighborhood centers, grocery stores, gas stations, restaurants, and homes – including vandalism, intimidation, assaults, and several murders.

In recent months, we have witnessed a disturbing number of violent assaults against legal and undocumented immigrants – and those perceived to be immigrants – by white supremacists and other far-right extremists. It is clear that extremist groups

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00126 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.001

are seeking to exploit national divisions over the nature of immigration reform to spread a message of xenophobia, promote hateful stereotypes, and incite bigotry and violence against Hispanics, regardless of their status as citizens.

The HCSA: A Firm Foundation on which to Build

The organizations listed below have worked to promote comprehensive hate crime data collection efforts. The FBI has taken important steps to make the information reported to the Bureau accessible to researchers, law enforcement officials, civic leaders, and community relations professionals. In 1996, for the first time, the FBI incorporated an HCSA summary report within its annual *Crime in the United States* (CIUS) report. Because CIUS is a primary resource for criminologists, policymakers, and analysts, inclusion encourages researchers and criminologists to study hate violence, helps place it on the agenda for criminal justice and crime prevention conferences, and sends the signal to law enforcement officials that the HCSA is a permanent, integral part of the FBI's comprehensive crime data collection programs.

In addition, the publication of the annual jurisdiction-by-jurisdiction report, *Hate Crime Statistics,* has been especially useful in helping to gauge the seriousness with which communities and police departments are approaching the Federal hate crime data collection effort. For example, in 2004, the most current jurisdiction-by-jurisdiction information available, seven states (Alabama, Alaska, Hawaii, Mississippi, North Dakota, South Dakota, and Wyoming) reported 10 or fewer hate crime incidents. [http://www.fbi.gov/ucr/hc2004/openpage.htm] Hawaii did not participate in the HCSA program at all. In addition, of the 50 most populous cities in the U.S., three did not participate in the reporting of hate crime data at all: Detroit, Indianapolis, and Honolulu. Other large cities were, apparently, deficient in their HCSA reporting. Miami and Oklahoma City affirmatively reported zero hate crimes to the FBI. The reporting in the following cities, all among the 50 most populous cities in the U.S, was notably questionable. The number of incidents is reported in parenthesis:

Houston, TX (14) - 4th largest
Philadelphia, PA (20) - 5th largest
Jacksonville, FL (3) - 13th largest
Austin, TX, (5) - 16th largest
Memphis, TN (1) - 17th largest
Forth Worth, TX (11) - 19th largest
Charlotte, NC (8) - 20th largest
El Paso, TX (8) - 21st largest
Milwaukee, WI (2) - 22nd largest
Denver, CO (7) - 25th largest
Nashville, TN, (5) - 28th largest
New Orleans, LA (6) - 35th largest
Kansas City, MO (2) - 40th largest
Omaha, NE (5) - 43rd largest
Oakland, CA (3) - 44th largest
Miami, FL (0) - 46th largest

Despite this seemingly incomplete reporting record over the first fourteen years of the Act, the HCSA has proved to be a powerful mechanism to confront violent bigotry against individuals on the basis of their race, religion, sexual orientation, disability, or ethnicity. Importantly, the HCSA has also increased public awareness of the problem and sparked improvements in the local response of the criminal justice system to hate violence. For example, in recent years, dozens of law enforcement agencies across the country have promulgated new policies and procedures for

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00127 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.002

addressing hate violence. Building on model policies drafted by, among others, the International Association of Chiefs of Police and the National Organization of Black Law Enforcement Executives (NOBLE), departments have complemented their participation in the HCSA data collection initiative with the development of protocols for their officers on how to identify, report, and respond to hate violence.

Police officials across the country have come to appreciate the law enforcement and community benefits of tracking hate crime and responding to it in a priority fashion. Law enforcement officials now better understand that they can advance police-community relations by demonstrating a commitment to be both tough on hate crime perpetrators and sensitive to the special needs of hate crime victims. By compiling statistics and charting the geographic distribution of these crimes, police officials may be in a position to discern patterns and anticipate an increase in racial tensions in a given jurisdiction.

The obstacles to comprehensive reporting, however, are significant. Studies by NOBLE and others have revealed that some of the most likely targets of hate violence are the least likely to report these crimes to the police. In addition to cultural and language barriers, some immigrant victims, for example, fear reprisals or deportation if incidents are reported. Many new Americans come from countries in which residents would never call the police -- especially if they were in trouble. Gay, lesbian, transgender, and bisexual victims, facing hostility, discrimination, and, possibly, family pressures because of their sexual orientation and gender identity, may also be reluctant to come forward to report these crimes. These issues present a critical challenge for improving law enforcement response to hate violence. When police departments implement the HCSA in partnership with community-based groups, the effort should enhance police-community relations.

Specific Recommendations for Improvements

1) **The Hate Crime Incident Report should be revised to provide space to encourage additional narrative about the bias motivation present.** The facts surrounding these crimes are all-important in determining whether the crime was, in fact, motivated by bias. Responding officers should be encouraged to provide relevant background information that documents why he or she believes the crime to be bias motivated – and space should be allocated to it on the Hate Crime Incident Report form.

Professor Jack McDevitt, Director of The Center for Criminal Justice Policy Research at Northeastern University, has also stressed the need for an expanded narrative in reporting hate crimes. In his September 2002 report, "Improving the Quality and Accuracy of Bias Crime Statistics Nationally," funded by the Justice Department's Bureau of Justice Statistics, McDevitt suggested that more detailed reporting can reduce the occurrence of "information disconnect" between the investigating officer and UCR reporting officials.

2) **The Hate Crime Incident Report should provide additional specificity in the Bias Motivation section, under Ethnicity/National Origin.** The current form provides a box only for "Anti-Hispanic" and "Anti-Other Ethnicity." The FBI report, Hate Crime Statistics 2001, [http://www.fbi.gov/ucr/01hate.pdf] documented that the number of hate crimes directed at individuals on the basis of their national origin/ethnicity doubled -- from 911 in 2000 to 2,098 in 2001. Although we do not know exactly how many of the 2001 reported hate crimes were "backlash incidents" directed at individuals in the aftermath of the September 11 terrorist attacks, it seems clear that a considerable portion of the dramatic increase in these crimes were in

38189.003

connection with bias-motivated attacks against individuals who "looked like" the terrorists. We strongly recommend that the FBI include one other box in this section for "Anti-Arab" crimes. At a minimum, however, the "Anti-Other Ethnicity/National Origin" line should include a line that includes "Anti-Arab," the "Religion" section should include a line for "Anti-Sikh" and "Anti-Hindu," and the "Sexual Orientation" section should include "Anti-Transgender" as examples of such crimes.

3) **The revised Hate Crime Incident Report should include a box in the Bias Motivation section for gender-based hate crimes.** As states continue to enact hate crime statutes, the clear trend has been to include gender-based crimes in these laws. In 1990, only seven of the statutes in the thirty-one states which then had hate crime statutes included gender. Today, including the District of Columbia, twenty-eight of the forty-six states with penalty-enhancement hate crimes statutes include gender. Nine states, including the District of Columbia, now include gender in their hate crime data collection mandate. Gender-based crimes are also subject to Federal sentencing enhancements under 28 U.S.C. 994.

4) **The revised Incident Report should provide a place for the race, religion, national origin/ethnicity, gender, and age of both the victim and the suspected offender.** Where it is readily obtainable, the personal characteristics of the suspected offender, as well as the victim, would be highly relevant facts to include in the Hate Crime Incident Report. Age information would be especially useful in efforts to learn more about juvenile hate crime offenders and victims. The FBI's annual HCSA report does not currently provide specific information about either juvenile hate crime offenders or victims. There is, in fact, a paucity of information about juvenile involvement in hate violence. A 1996 Department of Justice Office of Juvenile Justice Delinquency Prevention "Report to Congress on Juvenile Hate Crime" stated: "...the research team found very little information pertaining to the issue of hate crimes in general and even less on the nature and extent of juveniles' involvement." *Report to Congress on Juvenile Hate Crime,* July, 1996.

A September, 2001 Department of Justice Bureau of Justice Statistics Special Report, *Hate Crimes Reported in NIBRS, 1997-99* [http://www.ojp.usdoj.gov/bjs/abstract/hcrn99.htm] closely examined about 3,000 of the almost 24,000 hate crimes reported to the FBI during that period and found that 60% of the hate crimes reported under the incident-based system were violent crimes, while only 20% of the other incident-based reports were violent crimes. That report provided disturbing information about the too-frequent involvement of juveniles in hate crime incidents. The report documented that a disproportionately-high percentage of both the victims of hate violence and the perpetrators were young people under 18 years of age:

- 33% of all known hate crime offenders were under 18, including 31% of all violent crime offenders and 46% of the property offenders.
- Another 29% of all hate crime offenders were 18-24.
- 30% of all victims of bias-motivated aggravated assaults and 34% of the victims of simple assault were under 18.
- 34% of all persons arrested for hate crimes were under 18, including 28% of the violent hate crimes and 56% of the bias-motivated property crimes.
- Another 27% of those arrested for hate crimes were 18-24.

5) **The revised Hate Crime Incident Report form should be accompanied by the distribution of a revised and updated Training Guide for Hate Crime Data Collection.** The last revision of this document and its companion, Hate Crime Data Collection Guidelines, was in 1996. The revised Guidelines and Training Guide

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.004

should be more inclusive -- including examples of hate crimes directed against Arabs, Sikhs, Hindus, members of the transgender community, and women.

6) **The FBI should take specific actions designed to improve training and outreach for campus law enforcement authorities to help improve college and university HCSA reporting.** As indicated in the attached chart, participation in the HCSA data collection effort by campus law enforcement authorities at some of the nation's best-know colleges and universities has been quite deficient over the past five years.

In addition to these six specific recommendations, here are several other policy recommendations and revisions that our coalition plans to promote to help expand participation in the HCSA initiative:

**** The Administration and Congress should take steps to ensure that the FBI receives sufficient funding to continue to respond to requests for hate crime training from law enforcement agencies across the country, as well as funding to continue its own training and education outreach efforts for both new agents and in-service training for field agents at its Quantico training academy.** The FBI has been receptive to requests for HCSA training for state and local law enforcement officials in the past. Groups with expertise in analyzing and responding to hate violence have participated in a number of these training seminars for state and local law enforcement authorities on how to identify, report, and respond to hate crimes.

**** The Justice Department should make participation in the HCSA program a prerequisite for receiving funds to hire new officers and to receiving other Federal technical assistance and training grants.**

**** The Justice Department and the FBI should provide additional incentives for HCSA implementation, including national recognition, matching grants for training, a network to promote replication of successful programs, and awards for exemplary departments.**

**** FBI Field Offices should be encouraged by Headquarters to work more closely with police departments in their jurisdictions to promote participation in the HCSA reporting effort.** Collecting data under the HCSA – and training officers to identify, report, and respond to acts of violence based on prejudice – demonstrates a resolve to treat these inflammatory crimes seriously. These positive steps can be amplified by involving representatives of minority communities in the training sessions.

Especially at this time of increased terrorist threat, we welcome the continuing efforts of the Bureau to spark improvements in the response to an especially consequential form of domestic terrorism – hate violence. We look forward to continuing our partnership with the FBI in support of education and outreach efforts to improve the response to hate violence in America.

Sincerely,

American Association of University Women
American Jewish Committee
American Psychological Association (APA)
American-Arab Anti-Discrimination Committee (ADC)

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.005

Americans for Democratic Action
Anti-Defamation League
The Arc of the United States
Asian American Justice Center (AAJC)
Asian Pacific American Legal Center of Southern California (APALC)
B'nai B'rith International
Center for the Study of Hate & Extremism, California State University, San Bernardino
GLSEN -- the Gay, Lesbian and Straight Education Network
Hadassah, The Women's Zionist Organization of America
Hindu American Foundation (HAF)
Human Rights Campaign
The Interfaith Alliance
Japanese American Citizens League
Jewish Council for Public Affairs
Leadership Conference on Civil Rights
League of United Latin American Citizens (LULAC)
Mexican American Legal Defense and Educational Fund (MALDEF)
NA'AMAT USA
National Association for the Advancement of Colored People (NAACP)
The National Center for Transgender Equality
National Coalition for the Homeless
National Council of Jewish Women
National Council of La Raza
National Gay and Lesbian Task Force
National Urban League
North American Federation of Temple Youth
Organization of Chinese Americans
Parents, Families and Friends of Lesbians and Gays (PFLAG)
People For the American Way
Religious Action Center of Reform Judaism
Sikh American Legal Defense and Education Fund (SALDEF)
The Sikh Coalition
Society for the Psychological Study of Social Issues (SPSSI)
Unitarian Universalist Association of Congregations
United Cerebral Palsy
United States Students Association Foundation
United Synagogue of Conservative Judaism
YWCA USA

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.006

October 23, 2006

The Honorable Robert S. Mueller, III
Director
Federal Bureau of Investigation
935 Pennsylvania Ave., NW
Washington, DC 20535

Dear Mr. Mueller:

On behalf of the broad coalition of civil rights, education, law enforcement, religious, professional, and civic organizations listed below, we are writing to express our concerns that the 2005 edition of *Crime in the United States* was published without a summary of hate crime data. This is the first year since 1996 that the Bureau's essential crime data research tool has not included summary hate crime statistics.

We urge you to reconsider the decision to remove the summary hate crime data from *CIUS*. Because *CIUS* is a primary resource for criminologists, policymakers, and analysts, inclusion encourages researchers and criminologists to study hate violence, helps place it on the agenda for criminal justice and crime prevention conferences, and sends the unmistakable signal to law enforcement officials that the HCSA is an integral part of the FBI's comprehensive crime data collection, tracking, and analysis programs. As you know, Congress designated hate crime as a permanent mandate within the UCR Program in the Church Arson Prevention Act of 1996 (Public Law No. 104-155).

We are aware that the Bureau has now released hate crime statistics as a separate-standing report. That annual jurisdiction-by-jurisdiction report is essential – and has been especially useful in helping to gauge the seriousness with which communities and police departments are approaching the Federal hate crime data collection effort.

However, omitting summary hate crime data in this year's online edition of *CIUS* – with a month delay before the availability of hate crime data – sends the wrong message at the wrong time to both law enforcement agencies and victim assistance groups. In 2005, only 12,417 of the more than 17,000 city, county, state, tribal, and federal law enforcement agencies participated in the HCSA data collection effort. Included among the thousands of police agencies that did not participate in the HCSA data collection effort were two of the largest cities in America – New York and Phoenix. Moreover, the vast majority of the participating agencies affirmatively reported zero hate crimes to the Bureau; only about sixteen percent of the participating agencies reported a single hate crime. This inadequate level of law enforcement participation demonstrates the need to promote both increased participation in the overall HCSA data collection effort and more accurate reporting.

Many of the organizations listed below have worked closely with the FBI over the years to promote comprehensive hate crime data collection and training efforts. In the aftermath of the enactment of the HCSA, we helped the FBI design its thoughtful, inclusive hate crime data collection guidelines and training manuals. Representatives of many of our groups have

38189.007

participated in FBI-sponsored training programs on the topic for law enforcement agencies and community groups.

The urgent national need to be prepared to confront violent bigotry has only increased since the September 11, 2001 terrorist incidents. As you know, in the immediate aftermath of the September 11 terrorism, the nation witnessed a significant increase in attacks against American citizens and others who appeared to be of Muslim, Middle Eastern, and South Asian descent. And in recent months, we have witnessed a disturbing number of violent assaults against legal and undocumented immigrants – and those perceived to be immigrants – by, among others, white supremacists and other far-right extremists. At this time, as many of our organizations work closely with community-based groups and victim advocacy organizations to overcome obstacles for victims of hate crimes to come forward to report these incidents to the police, we must ensure that the data collected will be broadly accessible for policymakers and law enforcement officials.

Since 1990, the FBI has demonstrated a strong commitment to make hate crime data accessible to researchers, law enforcement officials, civic leaders, and community relations professionals. The HCSA has proved to be a powerful mechanism to confront violent bigotry against individuals on the basis of their race, religion, sexual orientation, disability, or ethnicity. The Bureau's good work in implementing the HCSA has increased public awareness of the problem – and sparked essential improvements in the local response of the criminal justice system to hate violence. In recent years, dozens of law enforcement agencies across the country have promulgated new policies and procedures for addressing hate violence. Building on model policies drafted by, among others, the International Association of Chiefs of Police and the National Organization of Black Law Enforcement Executives (NOBLE), departments have complemented their participation in the HCSA data collection initiative with the development of protocols for their officers on how to identify, report, and respond to hate violence.

After fifteen years of progress, we should be doing more to promote improved hate crime response, reporting, and training – not less. We urge you to update the online version of *CIUS 2005* with references to the 2005 hate crime data – and we urge you to ensure the fullest possible integration of hate crime data as a permanent part of *CIUS*, the Law Enforcement National Data Exchange System, and other FBI and Justice Department online criminal justice databases as they evolve in the years to come.

Sincerely,

American-Arab Anti-Discrimination Committee (ADC)
American Association of University Women
American Civil Liberties Union
Americans for Democratic Action
American Jewish Committee
American Jewish Congress
Anti-Defamation League
Asian American Justice Center
Asian Pacific American Legal Center of Southern California
B'nai B'rith
Center for New Community

Center for the Prevention of Hate Violence
Center for the Study of Hate & Extremism, California State University, San Bernardino
The Episcopal Church
GLSEN -- the Gay, Lesbian and Straight Education Network
Hadassah, the Women's Zionist Organization of America
Human Rights Campaign
The Interfaith Alliance
International Brotherhood of Teamsters
Japanese American Citizens League
Jewish Council on Public Affairs
Lawyers' Committee for Civil Rights Under Law of the Boston Bar Association
Leadership Conference on Civil Rights
Log Cabin Republicans
Mexican American Legal Defense and Education Fund
NAACP
National Association for Multicultural Education (NAME)
National Center for Transgender Equality
National Coalition for the Homeless
National Council of La Raza
National Council of Jewish Women
National Education Association
National Gay and Lesbian Task Force
National Organization of Black Law Enforcement Executives (NOBLE)
National Sheriffs' Association
National Urban League
North American South Asian Bar Association (NASABA)
Organization of Chinese Americans
Parents Families and Friends of Lesbians and Gays (PFLAG)
People For the American Way
Police Executive Research Forum (PERF)
Police Foundation
Presbyterian Church (USA), Washington Office
Religious Action Center of Reform Judaism
Sikh American Legal Defense and Education Fund (SALDEF)
Southern Poverty Law Center
Unitarian Universalist Association of Congregations
United Church of Christ, Justice and Witness Ministries
United Jewish Communities
United States Student Association
YWCA USA

U.S. Department of Justice

Federal Bureau of Investigation

Clarksburg, WV 26306

November 30, 2006

Anti-Defamation League
Suite 1020
1100 Connecticut Avenue, N.W.
Washington, DC 20036

Dear Ladies and Gentlemen:

Your October 23 letter to Director Robert S. Mueller, III, expressing concern about the removal of preliminary hate crime statistics from the FBI's annual report *Crime in the United States, 2005*, was forwarded to the Criminal Justice Information Services (CJIS) Division, where the Uniform Crime Reporting (UCR) Program is administered, for a response.

As detailed in your letter, preliminary hate crime statistics were added to *Crime in the United States* beginning with the 1996 edition. With the 2005 Uniform Crime Reports, the FBI exclusively published UCR data electronically. Because there were no hard copies of these publications, the FBI seized the opportunity to examine the data provided in the Uniform Crime Reports and to pursue ways the data could be more effectively presented in the Internet environment.

In redesigning the UCR publications, the FBI made the decision to remove the preliminary hate crime data from *Crime in the United States* for the following reasons:

1) The hate crime statistics were the only preliminary data in a report that otherwise featured final published numbers.

2) The conversion from hard copy to Web publications facilitated more efficient production of the Uniform Crime Reports. In addition, it enabled the FBI to release final data earlier than in previous years because there was no lengthy printing delay. The 2005 edition of *Hate Crime Statistics*, which contains final data for the year, was released about a month earlier than in previous years, and within a month of *Crime in the United States, 2005*.

3) The UCR Program administrators believed that the preliminary release of hate crime data in *Crime in the United States* lessened the impact of the release of the final data published in *Hate Crime Statistics*.

Anti-Defamation League

The decision to remove the preliminary hate crime data from *Crime in the United States* was reviewed by the CJIS Advisory Policy Board (APB). The redesigned *Crime in the United States* was presented at the APB's UCR Subcommittee meeting in San Antonio, Texas, in April 2006 and then to the entire APB in Cincinnati, Ohio, in June 2006. Subcommittee and APB members raised no objections to the change at either meeting. Also, an illustrative Web site demonstrating the "retooled" version of the publication was placed on the Law Enforcement Online Intranet for review and comment by law enforcement leaders. At that time, our law enforcement partners offered no feedback regarding the removal of the preliminary hate crime data from *Crime in the United States*.

Although the decision to exclude preliminary hate crime data from *Crime in the United States* was well thought out and thoroughly reviewed, we understand the concerns expressed in your letter. In response, the FBI will work to better align hate crime statistics with *Crime in the United States, 2006*, thus giving hate crime data more visibility in conjunction with this publication.

The FBI takes its administration and stewardship of the UCR Program and all its components, including hate crime data collection, very seriously. As you are aware, the FBI is currently taking a comprehensive look at ways to revitalize the hate crime program. As you indicated in your letter, many of the organizations you listed have worked closely with the FBI over the years to promote and improve the collection and reporting of the data. We appreciate your interest and work in improving and invigorating the hate crime data collection program.

Thank you for your comments and concerns. During this evolution of our publications from paper-based to Internet-based products, as well as the continued development of our data collection processes, we greatly appreciate the feedback of all stakeholders in the FBI's UCR Program.

Sincerely yours,

Thomas E. Bush, III
Assistant Director
Criminal Justice Information
Services Division

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00136 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.011

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 23, 2005

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

Dear Mr. Chairman:

On Sunday, November 6, the *Washington Post* published a feature article by Barton Gellman titled "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans." The article presents a materially misleading portrayal of the FBI's use of National Security Letters (NSLs), which are a long-standing and important tool for preventing terrorist attacks and espionage. Contrary to the impression created by the *Post*'s article, NSLs do not empower the FBI to spy on ordinary Americans, to listen to phone calls or read emails, or to review what books Americans read or web sites they visit. Rather, NSLs empower the FBI to conduct national security investigations by requesting very specific categories of information critical in tracking the activities of terrorists and spies and determining whether a person is a terrorist or spy.

While many of the distortions and factual errors in the *Post*'s article can be debunked only through classified information, other flaws in the article's discussion are revealed on the face of public records and of the laws passed by the Congress. Indeed, some are revealed in the article's own internal inconsistencies. We have already briefed your staffs on many of the article's distortions and falsehoods, including those for which the underlying facts are classified. This letter is intended to provide you an account of the facts regarding certain inaccuracies that can be rebutted in an unclassified format. We have therefore listed a number of those errors and explained the truth regarding those errors.

1. **As a general theme, the *Post* claims that the FBI uses NSLs to spy on law-abiding Americans. This is simply false: The FBI cannot and does not use NSLs outside of authorized national security investigations.**

   Claims: "The PATRIOT Act, and the Bush administration guidelines for its use, transformed those [national security] letters by permitting clandestine scrutiny of U.S. residents and visitors who are not alleged to be terrorists or spies."; "Career investigators and Bush administration officials emphasized, in congressional testimony and interviews for this story, that national security letters are for hunting terrorists, not fishing through the private lives of the innocent. The distinction is not as clear in practice."

Fact: **By law and in practice, NSLs cannot be and are not used to spy on law-abiding Americans or to investigate ordinary crimes or even domestic terrorism — they are limited to requests for information relevant to authorized investigations of international terrorism and espionage.** To be sure, some people whose records are produced in response to an NSL may not be terrorists or spies or associated with terrorists or spies. But in these vital investigations, the FBI needs to be able to check out every tip and track down every lead. As the attacks of 9/11 taught us all, even the slightest lead must be aggressively pursued. NSLs allow the FBI use of an efficient tool for determining the seriousness of the threat posed by suspected terrorists or spies and their associates — including the ability to cull unwitting acquaintances from complicit and dangerous co-conspirators.

2. **The *Post* insinuates that the FBI uses NSLs to seek library patrons' check-out records and monitor visits to disfavored websites. But the statutes authorizing NSLs do not authorize the FBI to request information on "the books [library patrons] borrow" or to monitor traffic on websites, and the FBI complies with those statutes.**

Claims: "[T]he vendors of the software he operates said their databases can reveal . . . the books they borrow. [The purported NSL recipient] refused to hand over those records . . . ."; "If the government monitors the Web sites that people visit and the books that they read, people will stop visiting disfavored Web sites and stop reading disfavored books."

Fact: **The FBI by law cannot, and in practice does not, request that an NSL recipient disclose e-mail contents or library checkout records.** The NSL statutes strictly limit what information may be requested, and from whom. The NSL in the Connecticut case was issued under 18 U.S.C. § 2709, which does not authorize requests for book borrowing records. Indeed, despite the *Post*'s insinuation, the *Post*'s own description of the NSL at issue in the Connecticut case (the accuracy of which can only be discussed in a classified setting) does not suggest that the FBI sought check-out records. Justice Ginsburg's opinion denying emergency relief in that case confirms this, characterizing the NSL as requesting "'subscriber information, billing information[,] and access logs'" — not book check-out records. *Doe v. Gonzales*, 546 U.S. ___, No. 05A295 (Oct. 7, 2005) (Ginsburg, J., in chambers). As for websites, tracking visits to websites cannot be done under an NSL.

3. **The *Post* implies that NSLs are left entirely to the FBI's discretion. In doing so, the *Post* ignores robust mechanisms for checking misuse.**

Claim: "They [NSLs] receive no review after the fact by the Justice Department or Congress."

Fact: **FBI NSL usage is subject to Justice Department and Congressional oversight.** First, no NSL may be issued except in an authorized national security investigation, and no national security investigation may be authorized without notice to the Justice Department's Office of Intelligence Policy and Review and its Criminal Division. Second, should there be an allegation of wrongdoing involving an NSL, the Justice Department's Inspector General is empowered to investigate, and any misuse must be reported to the Intelligence Oversight Board. Third, all but one of the statutes authorizing use of NSLs require the FBI to "fully inform" Congress regarding the FBI's use of NSLs.

4. **The *Post* fundamentally mischaracterizes a recent Executive Order to claim that it requires the FBI to share private records of innocent Americans with entities outside the federal government.**

Claim: "Late last month, President Bush signed Executive Order 13388, expanding access to those files for 'state, local and tribal' governments and for 'appropriate private sector entities,' which are not defined."

Fact: **Executive Order 13388 does not give state, local, tribal, or private entities access to information gleaned from NSLs.** The Executive Order's reference to those entities directs that they be included in a federal project to bolster the "interchange of terrorism information" insofar as it is consistent with "the freedom, information privacy, and other legal rights of Americans." E.O. 13388 § 1. This policy directive implements section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which requires the sharing of terrorism information with "all appropriate Federal, State, local, and tribal entities, and the private sector." The information-sharing project includes policies and procedures to determine who is an appropriate recipient of what information, and to safeguard privacy and civil liberties. For instance, including private sector entities in the "interchange of terrorism information" will allow terror threat information to be shared, as appropriate, with business and critical infrastructure entities. There is no requirement that those entities be given access to information on innocent Americans.

5. **The *Post* implies that the FBI can use an NSL to compel production of private records without the intervention of a court, and that PATRIOT Act conferees are set to expand that authority. Neither contention has any basis in fact.**

Claim: "House and Senate conferees are poised again to amplify the FBI's power to compel the secret surrender of private records."

Fact: **The FBI cannot compel compliance with an NSL without seeking judicial intervention.** An NSL is not a court order or a grand jury subpoena; it is a request for records. In the event a recipient objects to the request, production can only be "compelled" by a court. Neither the House nor the Senate reauthorization bill contains language that would "amplify" existing NSL authorities. The changes supported by the Administration will create significant additional oversight and explicit procedures for judicial review — facts literally ignored by the *Post*.

6. **The *Post* implies that Congressional oversight of NSLs is inadequate and that, in any event, the Justice Department has failed to report how many NSLs it uses. To the contrary, the Justice Department provides Congress information on NSL usage in a number of forms, including reporting, briefings, and testimony.**

Claim: "The Justice Department has offered Congress no concrete information, even in classified form, save for a partial count of the number of letters delivered."; "As national security letters have grown in number and importance, oversight has not kept up."

Fact: **The Department of Justice has complied with thorough Congressional oversight of NSL use.** In addition to providing to Congress all information required by the numerous statutory reporting requirements regarding NSLs, the Department has participated in multiple hearings that addressed NSL authorities, responded to numerous written congressional queries, and conducted several classified briefings. It is simply false to suggest that the Justice Department has offered Congress "no concrete information" on NSL usage or that Congress has ignored its oversight responsibilities. Moreover, the article's denigration of the oversight the Congress can provide based on numbers of NSLs issued is unwarranted. The Department reports both the total number of NSLs issued and, most important, the number of different U.S. persons whose records the FBI has requested through NSLs. Those statistics permit Congress to see if there have been significant increases in the use of NSL authority. By way of example, if the *Post* is correct that NSLs were used during the Las Vegas investigation (a point we can neither confirm nor deny in an unclassified setting), our reports to Congress would include a huge number of U.S. persons, which would undoubtedly attract Congressional attention.

7. **The *Post* draws misleading and erroneous distinctions between NSLs and their criminal investigative counterpart, grand jury subpoenas.**

Claim: "Grand juries tend to have a narrower focus because they investigate past conduct, not the speculative threat of unknown future attacks. Recipients of grand jury subpoenas are generally free to discuss the subpoenas publicly."

Fact: **The distinctions the *Post* is attempting to draw between grand jury subpoenas and NSLs appear to be based on a fundamental misunderstanding of the grand jury process.** First, a grand jury subpoena certainly could be used to investigate "the speculative threat of unknown future attacks": grand juries are fully empowered to investigate ongoing conspiracies. Second, while grand jury subpoenas are available to investigate a wide range of criminal activities, NSLs are available only in authorized national security investigations, in which confidentiality is often a paramount concern. Finally, courts have repeatedly recognized that individuals do not have a First Amendment right to disclose information learned only by virtue of participation in an investigation, particularly where the national security is implicated.

8. **The *Post* incorrectly implies that then-Attorney General Ashcroft empowered the FBI to investigate terrorism without regard to Americans' civil rights and civil liberties.**

Claim: "He gave overriding priority to preventing attacks by any means available."

Fact: **The FBI must and does conduct its investigations within the bounds of our Constitution, statutes, strict internal guidelines, and Executive Orders.** Attorney General Ashcroft did not authorize, and could not have authorized, the FBI to disregard those constraints. It is simply false to suggest that there are no legal restrictions on the FBI's investigations, even of terrorism.

9. **The *Post* asserts that because subjects are not notified of the issuance of an NSL, no one can challenge that issuance. This contention is wrong, given the availability of various oversight mechanisms and judicial review.**

Claim: "Because recipients are permanently barred from disclosing the letters, outsiders can make no assessment of their relevance . . . ."

Fact: **Recipients can challenge NSLs in court. Moreover, they can notify the Justice Department's Inspector General about perceived abuses. And NSL usage is subject to extensive Congressional oversight.** Any recipient can challenge the NSL it receives, and the courts and the Justice Department's Inspector General are all available to address those challenges. The Department takes the position that the nondisclosure requirement does not bar *all* disclosure but rather allows disclosure to an attorney. Moreover, NSLs are not self-enforcing; the FBI cannot compel compliance absent a federal court order. Finally, Congress conducts rigorous oversight over NSL usage. In short, the idea that there is no outside oversight of the FBI's NSL usage is simply wrong.

The Honorable Arlen Specter
Page Six

10. The *Post* erroneously implies that the permanent nondisclosure requirements do not serve a legitimate national security purpose.

Claim: "[N]ational security seldom requires that the secret be kept forever."

Fact: **Protecting the secrecy and integrity of national security investigations, techniques, and methods is critical to our ability to protect Americans from terrorist attacks and espionage.** The nondisclosure requirement serves two ends in national security investigations: (1) it prevents the target of an investigation from being tipped off; and (2) it ensures that we are not revealing too much information about our investigative capabilities and techniques to our enemies. It is the second reason in particular that the *Post* essentially ignores. There are many parties around the world who employ sophisticated techniques for gauging our intelligence and counterterrorism capabilities. Courts have repeatedly recognized the danger of publicly revealing information that in isolation appears harmless but when combined with other information provides our enemies insights into our capabilities and techniques. The nondisclosure requirement ensures that it is the FBI or the Justice Department that makes the determination whether information can be disclosed without harm to the national security or ongoing investigations. That decision is not one properly given to the recipient of an NSL, who will almost never be in a position to make that determination accurately.

11. The *Post* implies that the standard governing NSL use is toothless, ignoring the robust, binding legal guidance that informs that standard.

Claim: "To establish the 'relevance' of the information they seek, agents face a test so basic it is hard to come up with a plausible way to fail."

Fact: **By law, NSLs are limited to requests for information relevant to international terrorism and espionage investigations, and the FBI does not use them except in those authorized circumstances.** NSLs are not available to investigate ordinary criminal activity or even domestic terrorism. Moreover, the term "relevance" is one that has been employed in the law for generations — in fact, it is the standard for the issuance of a grand jury subpoena. It is simply false to suggest that "relevance" is an undefined or limitless concept.

12. The *Post* peddles the notion that the existence of the authority to use NSLs is itself an "abuse," regardless of how lawfully they are used. But the lawful use of a Congressionally authorized investigative tool is not an abuse.

Claim: "What the Bush administration means by abuse is unauthorized use of surveillance data — for example, to blackmail an enemy or track an estranged spouse. Critics are focused elsewhere . . . 'the abuse is in the power itself.'"

38189.017

Fact: **The Department of Justice takes seriously the limits on its authorities and fully understands that unlawful use of an authority is an abuse. But lawful use is by definition not abuse.** Contrary to the *Post*'s assertion, we do not limit our understanding of abuse to the egregious, such as blackmail or stalking. On the other hand, we do not agree — and neither should Members of Congress — that lawful and prudent use in appropriate circumstances of a duly authorized investigative authority itself constitutes "abuse."

13. **The *Post* implies that the nondisclosure requirement attaching to an NSL would prohibit the recipient from consulting an attorney, in spite of the Department's repeatedly stated position that the nondisclosure requirement does *not* prevent a recipient from seeking counsel.**

Claim: "He wanted to fight the FBI but feared calling a lawyer because the letter said he could not disclose its existence to 'any person.'"

Fact: **The NSL statute at issue in the Connecticut case allows disclosure of receipt to an "agent," which would include an attorney.** In practice, and in litigation, the Justice Department has repeatedly maintained that the nondisclosure requirement allows disclosure to an attorney. Moreover, the recipient *did* consult an attorney and *did* challenge the NSL, as evidenced by the *Post*'s own discussion of the lawsuit. The *Post* further ignores that the Department has expressed public support for legislation making explicit that a recipient may consult an attorney.

14. **The *Post* claims that the Department of Justice has hidden from the courts the facts underlying the Connecticut NSL case. This claim is simply baseless.**

Claim: "The central facts remain opaque, even to the judges, because the FBI is not obliged to describe what it is looking for, or why."

Fact: **The Department of Justice has fully complied with the courts' requests for the facts underlying the Connecticut case.** A comprehensive explanation was filed under seal; although the explanation is not publicly available, the judges have been fully informed. It is simply false to state that the FBI has withheld from the courts information on what the FBI is looking for and why. Moreover, with knowledge of the reason for the FBI's request, the District Court has not determined that the FBI's request is unreasonable or unwarranted; rather, the court only ruled that the law requires the availability of a challenge and prohibits a permanent nondisclosure provision. Neither of these rulings casts any doubt on the underlying validity of the FBI's request.

15. The *Post* incorrectly implies that a claim that businesses face dire consequences for noncompliance with government requests was directed to NSL requests.

Claim: The Post attributes to one expert the position that failure to comply with an NSL could mean that "a business could face criminal prosecution, 'a "death sentence" for certain kinds of companies.'"

Fact: **The Post failed to provide a single instance of the government prosecuting a business for failing to comply with a national security investigation.** This is unsurprising, as the government has never prosecuted any individual or company for failing to comply with an NSL. The Justice Department is not looking to impose the economic "death sentence" on businesses that fail to comply with NSLs, and the Post's suggestion to the contrary is irresponsible. The statements on which the Post bases its claim are taken out of context and did not, when made, refer to compliance with NSLs.

16. The *Post* incorrectly asserts that businesses have complained about the burden imposed by NSL requests.

Claim: "National security letters, [major business groups] wrote, have begun to impose an 'expensive and time-consuming burden' on business."

Fact: **The letter to which the *Post* refers did not single out NSLs as burdensome but instead indicated in general that "document requests from the government" can pose an "expensive and time-consuming burden."** There exist a variety of investigative tools with which the government can request documents from businesses, including the familiar grand jury subpoena. Many of these tools can impose substantial compliance burdens on businesses. But the *Post*'s misrepresentation that businesses groups singled out NSLs as expensive or time-consuming is simply false. Indeed, in the Justice Department's experience, NSLs are much *less* "expensive and time-consuming" for recipients than some other investigative tools, and nothing in the business groups' letter contradicts that understanding.

17. The *Post* also erroneously insinuates that there is no internal oversight of NSL usage.

Claim: "In the executive branch, no FBI or Justice Department official audits the use of national security letters to assess whether they are appropriately targeted, lawfully applied or contribute important facts to an investigation."

Fact: **The use of NSLs, like the use of any authority, is subject to significant internal oversight and checks.** As an initial matter, an NSL must be approved by a field office's Special Agent in Charge (SAC) or one of a handful of senior FBI headquarters officials — all members of the Senior Executive Service,

totaling fewer than 100 nationally. Before an NSL request even gets to the desk of an SAC, it will go through at least two levels of oversight, including legal compliance. After the fact, any misuse of an NSL is subject to significant oversight as part of the FBI's reports to the Intelligence Oversight Board. Finally, the Department of Justice Inspector General is empowered to investigate any allegations of abuse.

In addition to these corrections, we have provided classified briefings to your staffs, as well as to certain Members who requested them, regarding the following erroneous claims:

- "The FBI now issues more than 30,000 national security letters a year, . . . a hundredfold increase over historic norms."
- "The Bush administration . . . has offered no example in which the use of a national security letter helped disrupt a terrorist plot."
- "In late 2003, the Bush administration reversed a long-standing policy requiring agents to destroy their files on innocent American citizens, companies and residents when investigations closed."
- "Criticized for failure to detect the Sept. 11 plot, the bureau now casts a much wider net, using national security letters to generate leads as well as to pursue them."
- "Agents commonly use the letters now in 'preliminary investigations' and in the 'threat assessments' that precede a decision whether to launch an investigation."
- "Ashcroft remained bound by Executive Order 12333, which requires the use of the 'least intrusive means' in domestic intelligence investigations. But his new interpretation came close to upending the mandate."
- "Two years ago, Ashcroft rescinded a 1995 guideline directing that information obtained through a national security letter about a U.S. citizen or resident 'shall be destroyed by the FBI and not further disseminated' if it proves 'not relevant to the purposes for which it was collected.' Ashcroft's new order was that 'the FBI shall retain' all records it collects and 'may disseminate' them freely among federal agencies."
- "[T]he FBI had served national security letters on [Las Vegas casinos]. In an interview for this article, one former casino executive confirmed the use of a national security letter."

The Honorable Arlen Specter
Page Ten

The Department of Justice is committed to protecting civil liberties and to using all investigative tools judiciously and within the bounds of the law. This includes NSLs, which are one of the important tools Congress provided the Department to help us secure our nation. We urge the Congress not to let a distorted and misleading portrayal of the FBI's use of this vital investigative tool skew the debate over how best to ensure our national security.

If we can be of further assistance, please do not hesitate to contact this office.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

38189.021

United States Senate

WASHINGTON, DC 20510

March 22, 2007

Via Electronic Transmission

The Honorable Robert S. Mueller, III
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Mueller:

Last December, my staff discussed with FBI Congressional Affairs the possibility of quoting, in some questions for the record, portions of the transcript of the meeting at issue in the allegations of former Special Agent Michael German. The FBI's cover letter on the transcript stated in pertinent part the following:

> We have made every effort to release information relating to the Committee's oversight interest while still protecting law enforcement equities relating to sensitive sources, techniques and ongoing investigative interests . . . As with the material provided previously, these documents may contain information the public disclosure of which might be prohibited by the Privacy Act. We are providing them to the Committee in response to its oversight request and pursuant to 5 U.S.C. 552a(b)(9). We respectfully request that the Committee not further disseminate this information prior to consultation with the FBI.

My staff consulted with the FBI, as requested by the cover letter, and sought more specific guidance on which portions of the hundreds of pages of unclassified transcript were sensitive and why. FBI Congressional Affairs would not say whether there was currently an active investigation on either of the subjects in the transcript and refused to identify specific passages of concern. Instead, while raising no legal objections, the FBI took the position during these informal consultations that it would be inappropriate to quote *any* excerpts from the transcripts whatsoever.

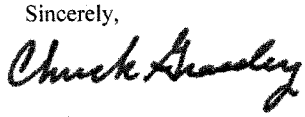
Small sections have been quoted from second-hand sources in a previous letter from Senator Leahy, Senator Specter, and me to the Justice Department's Inspector General. Moreover, the Inspector General quoted other selections from the transcript in his reply. Since then, however, the FBI has provided the entire transcript, and as a whole, it appears much more consistent with Special Agent German's descriptions than with the FBI's.

While I appreciate the FBI's efforts to provide this information and recognize its interests in protecting "law enforcement equities," the contrast between the discussions recorded in the transcript and the FBI's public claims about the meeting are stark and disturbing. It is hard to believe that every line on every page of the transcript is so sensitive that its disclosure would endanger an ongoing investigation or compromise the FBI's sources and methods. Questions about these conflicts need to be answered openly and on the public record.

Therefore, in order to facilitate that public discussion, please identify the specific passages that would compromise sensitive sources, techniques, or ongoing investigative interests and provide an explanation of why each passage is sensitive. In addition, please describe the history of the FBI's investigations involving the two subjects in the transcript, including: (1) the opening and closing dates of the investigations, (2) the potential offenses for which they were investigated, (3) whether the investigations resulted in any criminal charges, and (4) whether there is a pending investigation on either subject that is likely to result in criminal charges.

Please provide this information as soon as possible, so that this issue can be addressed as part of next week's FBI oversight hearing. If you have any questions about this request, please contact Jason Foster at (202) 224-4515. A copy of all correspondence in reply should be sent electronically in PDF format to thomas_novelli@finance-rep.senate.gov or via facsimile to (202) 228-2131.

Sincerely,



Charles E. Grassley
U.S. Senator

cc: Senator Patrick Leahy, Chairman
Committee on the Judiciary

Senator Arlen Specter, Ranking Member
Committee on the Judiciary

38189.023

United States Senate

WASHINGTON, DC 20510

March 26, 2007

Via Electronic Transmission

The Honorable Robert S. Mueller, III
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

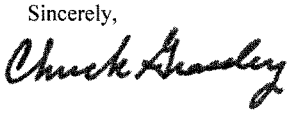
Dear Director Mueller:

On March 22, I wrote to you to regarding the transcript at issue in the dispute between former Special Agent Michael German and the FBI. I asked you to please identify any specific passages in the transcript that would compromise sensitive sources, techniques, or ongoing investigative interests and provide an explanation of why each passage is sensitive.

Having received no reply and heard no legal objections from the FBI, I am now writing to inform you that I may refer to or quote excerpts from that transcript at tomorrow's Judiciary Committee hearing or in questions submitted for the record. In particular, I may refer to or quote from one of the 14 excerpts detailed in the attached summary. In addition, I asked you several questions about the FBI's investigations involving the two subjects in the transcript, including whether there are any currently pending investigations. However, I have yet to be advised of any answers to those questions.

If you have any questions about this correspondence, please contact Jason Foster at (202) 224-4515. A copy of any reply should be sent electronically in PDF format to thomas_novelli@finance-rep.senate.gov or via facsimile to (202) 228-2131.

Sincerely,



Charles E. Grassley
U.S. Senator

Attachment

cc: Senator Patrick Leahy, Chairman
Committee on the Judiciary

Senator Arlen Specter, Ranking Member
Committee on the Judiciary

Consensual Monitor Transcript, January 23, 2002

1(WS) = Subject 1, White Supremacist
2(IM) = Subject 2, Islamic Militant
C = Cooperating Witness
UI = Unintelligible

	Trscpt 1, p.	Trscpt 2, p.	Excerpt/[*Comment*]
1	41-42		1(WS): Did you have an opportunity to meet with my associate? 2(IM): Uh, yeah. * * * 1(WS): Sure. 2(IM): So why not? Why shouldn't we stand for white person? O.K.. So you understand it. But I also conclude that the enemy of my enemy is my friend. 1(WS): That's where we're comin' from. 2(IM): O.K.? So whoever… Anybody that's willing to . . . to shoot a Jew or to hit a Jew is my friend. Automatically. (UI) is blood to the water. I mean, I … Nothing (UI). 1(WS): I understand.
2	44		2(IM): They [the Jews] own everything. You will not get a job unless you sleep with their daughter. That's the Germans before Hitler came. Everybody thinks Hitler is a… is a criminal… is a, a sick individual. The man was a genius. 1(WS): He was a hero for our people. 2(IM): He is a genius. He's my hero. The man was a genius. The man knew exactly what to do.
3	50-51	48(40)	2(IM): Our hope is we got a great country and we rely on that, Iran. 1(WS): They're comin' around. They sent you guys arms. 2(IM): Right. Iran (UI)… 1(WS): What I read about the ship. I liked. I can't.

38189.025

			But this is great. 2(IM): This not the first one.
4	56-57*	49-50	1(WS): So we cannot vote our way out of it. Americans can't. The way I look at it is this if you're gonna read the [*redacted white supremacist organization*] website and look at, at our strategy, it's clear. The only solution that we have is to replace the current government with a new government that's operating in the best interests of the American people. 2(IM): That'd be a long way to go. 1(WS): You're right. It's a long way to go, but you know what? We're moving in that direction. 2(IM): (UI) 1(WS): More and more people. 2(IM): Impossible. That would be next to impossible. 1(WS): I disagree. We started this country by fighting the most powerful regime on the planet to (UI). O.K.? The one thing that we need that we haven't fully developed, is more operational ties with your people because we have shared common goals … common goals. Now, we've talked about it in our circle. We've had serious conversations with the upper echelons, and I'm sure it must have come up in your circle too. But we've never really made concrete moves in that direction. The only way you guys can achieve your goals is by this country having a major shift in power. If you ever destabilized North America, you'd have a free hand over there. Do you follow what I'm saying? C: Man, we're not talkin' about anything uh, you know, radical or off the wall. It's gonna take work. Uh… And we're not talking about blowing up an Oklahoma… (UI). 1(WS): Oh no, some stupid shit like that. Man, we're talking about… C: Opening people's hearts and minds.

38189.026

			2(IM): You know, and… That's…the answer. Not changing the government but changing the people. (UI) This, this is (UI) democracy, uh, (UI). I mean I (UI) something here. But, I mean, I know no matter how much we have used that, we're tempted. But… I didn't know (UI). Sure enough, (UI) anywhere in the world, but when it comes to this country, (UI) my wars. I mean, I worship this country, but this country (UI). O.K.. But this country is in control. The wars really change the minds of the American people.
5	59-61	52-54	1(WS): The American people are never, ever on their own. They're gonna wake up one day and throw off the yoke (UI) that rule our country. They have to be steered in the right direction. And what the [*redacted white supremacist organization*] is doing… You've seen some of our literature. I think that's how you first came in contact with us. You saw the uh, (UI)… 2(IM): Mm hm. 1(WS): For Isreal. Do you know how many of those we distributed? Over five thousand households in got that. O.K.? * * * 2(IM): So what do you do? 1(WS): O.K., here's the deal…the gameplan. The organizational strategy for the [*redacted white supremacist organization*] is very simple. Recruit, organize, and activate as many of people as possible. We'll probably never get more than about five percent of 'em. United States population. But that's o.k.. But History's not made on majorities. Histories are made with minorities who have a majority of political will. Just like Hamas. Not everybody in the occupied territories has that determination, that will, to do what has to be done. Difficult decisions. You know, not everyone is a patriot to the level of the guys that have, you know, blowin' themselves up or planning these operations. Some people call

38189.027

			that criminal enterprise. I call it patriotism. 2(IM): Exactly. 1(WS): O.K.? We did the same thing to the British! You know what would have happened to George Washington if they would have caught him? 2(IM): I know. 1(WS): He was a terrorist, that's what they called him. 2(IM): Mm hm. 1(WS): They (UI) him as a patriot now. 2(IM): Exactly. * * * 1(WS): And I think in this country, it's gonna come down to that. I believe there's gonna be another civil war in this country. Now you can't say that maybe, but I will say that. * * * There is a sentiment out there…among real people who know it's coming. It'll have to happen. Now that's my problem. That's not your problem. I think it's my problem, you know? 2(IM): Anything that goes on in this country is our problem. Oh, we have to stick together. 1(WS): But what I'm saying is… What I'm saying is when I think of it that, this way, in terms of that, uh, civil war, I know that there is only one path towards breaking the power of the Jew. You will not get (UI) by voting him out of power. He's got a lock on the news of the media. You said it earlier in the conversation. The courts are corrupt. There is no justice in this country. His influence is dominant. 2(IM): Half of the… half of the (UI) are Jews. 1(WS): Oh yeah. 2(IM): (UI) ACLUs. 1(WS): And all of the media is Jewish.

38189.026

6	102-103*	90	2(IM): I do not believe in taking the human life…the innocent people's lives. 1(WS): Well, I'm not condoning that. What I'm telling you is the situation out there is now [*after 9/11*], more than ever Americans are paying attention to Middle Eastern policy. Now, most of them are still stupid. They still have wrong ideas. 2(IM): You know what he [*Bin Laden*] should have done? If I was him and with three hundred million dollars like he said. And I'm gonna say it frankly. O.K.. If he wants to do it militarily, he should have came over here and assassinate reporters of Israel. That's what I think (stutters) a more successful…peaceful. O.K.? He has… You know assassinates happen over (stutters) uh… resources (UI). He could have spent here three hundred million dollar cash and could have bought ABC…paid for it. He could have bought CNN.
7	113-115*	100-101	1(WS): Well, we're exposing the, the, the Holocaust story. Uh, what the main focus right now of our organization is breaking the power grip of the Jews in the United States. And the reason why we're here is because our goal of breaking the power grip of the Jews (UI) in the United States is the same…should be for your people, both over here and over there. If those guys over there were smart, and I think they are, they're doing pretty some interesting stuff. The first thing they would do is try to make, uh, contact with white nationalists and black nationalists too, but white nationalists that are opposed to the Jews controlling our destiny. * * * The worst threat to the Jews in America is this organization because they're not a bunch of Ku Klux Klan guys. There' even more effective than David Duke. [*Redacted*] but he's been marginalized. The game's now is to recruit as many people into the organization

38189.029

			and to build a revolutionary infrastructure. Infrastructure… Businessmen… People who own property… People who have influence…
			C: Politicians.
			1(WS): Behind us. And we're not asking you to step up and support [*redacted white supremacist organization*] in public. That'd be suicide for you to do. But we have front organizations, and we have enterprises that could benefit from assistance from you guys. Hook us up with other influential people from the Middle East. Um, let me give you an example. We've got uh uh a company that is the [*redacted*]. O.K., I'm gonna tell ya. I trust you. O.K.? (UI) But you obviously are not a sell-out. You have a Palestinian's beliefs. [*Redacted*] company is formed in [*redacted*]. It's brand new. We're about to get [*redacted*]. We're working on that right now. Because it's owned solely owned by [*redacted*]. Most of the guys who work there would be very comfortable in this conversation. We're recruiting some good ex-military people, getting good training by good guys… We're building this company. You think about that for a minute. Legitimately, we'll be trained. Legitimately, we'll be recruits. Legitimately we'll be able to, to give jobs to guys. I know a guy who lost his job because he said something against the Jews. Literally was fired because his boss was pressured by the Jews. Give a place for these people to go. O.K.? It doesn't need the Jews. Don't borrow a dime from the Jews. Provide uh… services. We've got some great ex-military people. O.K., good, solid ex-military people. We'd love to be in business with the Saudis who come over here or the Egyptians who come over here or the Palestinians that come over here. And they can know that this is not some Zionist guy. This is a guy who understands the real deal. They don't have to talk about it. But they know they're friendly forces. You understand what I'm saying? Um, network in business between these (UI)

38189.030

			2(IM): (UI) 1(WS): What's that? 2(IM): [*Redacted*] (UI) Saudis and those kind of people. 1(WS): Mm hm.
8	119-121*	104-106	1(WS): Now, what I'm, uh, tryin' to tell you about [*redacted*] is that these kinda outreaches… I've got another company. It's a [*redacted*] company. It's uh… My [*redacted*] and I are in, um, the business of making, um, [*redacted*]. He's come up with a [*redacted*]. O.K.? My… One of my dreams is to go immediately to Iraq and donate a bunch of it to them. O.K., it goes to Palestine, donate it a bunch of it to them. Go to Jordan when they have bad problems, sell it to them at a fair deal. Sell it to the Saudis, the people with money. You know? Build some … some talking, some trust. You know? Go to the Syrians. Go to Iran then. O.K.? Say, hey look, I'm American, but I'm an American who's got a brain, and I represent a lot of other guys underground that can't stick their head above water, but who sympathize with your cause, and we've got our other agenda in North America. And if we win, if our agenda is met, you guys got a home run. That's the basic message I wanted to bring to you. O.K.? * * * I had a heated debate with a gentleman in our organization. He's a little bit less sophisticated. You know what I'm saying? He was gonna go meet with (UI). Why are you gonna go meet with those Arabs? You know? What good can that do? You know they're, they're, they're not… They don't like you , you know, cuz you're white. Blah blah blah. I said, let me tell you something. If you gave us a couple hours time to sit down and beak some bread together, talked about it, build a bridge… I said, that's what the Jew fears the worst. Because he's not gonna be able to drive that split between us. O.K.? I'm

38189.031

			not gonna agree with you on every single one hundred percent thing. 2(IM): No. 1(WS): But I agree with you on enough things. They got (UI). 2(IM): They got the (UI). 1(WS): That's right. And have, and build operational links.
9	125	110	1(WS): You know, I just wanted to come today and extend an olive branch and say, hey look, we're you buddies. And if there's any way we can help you, we're there. And if there's any way you can help us, we wanna build those relationships. I was gonna tell ya about this. I made a contact with the um…recently, with the uh, [*redacted*] embassy. You know, I don't think that's the routed to take, I think I need to develop contacts in these governments and um, so every time I talk to someone… And I don't have a lot of friends that are Arab…that are of substance. You know? Uh, but I wanna get to those people.
10	134-135*	118-119	1(WS): [*Redacted*] is doing that now. You know one of the, one of the things I said earlier was that we're startin' to build front organizations. And we're building reach out and touchy kinds of things. It's, it's… [*redacted*] type of work for 'em is one of those. Um, we'd be happy to present our services to any of your people, you know, that are coming here to town. We'll give you good, you know, solid, reliable help. 2(IM): (UI) gonna do… I don't (UI) coming through, but if some of mine (UI). And uh, bus comes in, whatever, we try to (UI). O.K.. I'm gonna call 'em and talk to 'em and, and, and tell 'em that you (UI). * * * 1(WS): (UI) And I know you're busy. I just wanted to… You know, the, the first visit was just to

38189.032

			say hello. 2(IM): Thank you. 1(WS): Put another face on us. You met [*redacted*]. He's a very educated… 2(IM): Very nice.
11	137*		1(WS): I wanna increase the high level contacts with friendly people in this regime who think, who are anti-Zionists. If you can make introductions to me, fine. If you don't trust me enough yet, that's fine too, but I wanna move in that direction. I'd like to increase the bridged because you… 2(IM): You… You know, you know that there is a (UI) right now… 1(WS): Mm hm. 2(IM): Everything is just so dead. And people who are really active or this and that have kind of just vanished. This is the worst time. This is the worst time ever been for Arab Americans…the worst. For Arab Americans (UI). O.K.. It is the worst. (UI).
12	140		2(IM): I'll give you my card. My number is… 1(WS): We were so pleased when we heard you had the courage to call our message line from reading that pamphlet.
13	147		1(WS): Yeah, can you imagine what a hell it is to be an Israeli right now? 2(IM): Oh, in, in there? (UI) You live in the strongest country in the Middle East, but yet you're scared to ride the bus? You're scared to go to school? You're scared to go to your office. (UI). 1(WS): Tourism man. Guy got wasted in his own hotel hall. That was great by the way. 2(IM): Oh yeah!
14	154		1(WS): I've got a… I've got [*redacted*]. I'll let you get 'em for free. If anyone's ever hassling

38189.033

			you here.. 2(IM): No. No. 1(WS): Call us. We'll send 'em over. You know, if you've ever got a problem. 2(IM): (UI) guards to… (UI) I like to participate in many things that I can be allowed to do (UI). 1(WS): Sure. Sure. Well, we'll…be glad to teach you.

Statement of Senator Edward M. Kennedy on FBI Oversight

March 27, 2007

We all agree that federal law enforcement and intelligence officers should have the techniques and resources they need to investigate terrorism and prevent future attacks. They also need to be able to share information with state and local law enforcement.

But the American people deserve to know whether this power is being used properly.

The PATRIOT ACT, which we reauthorized last year, includes controversial provisions which, if misused, have the potential to undermine important civil liberties. These provisions gave the FBI significant power to obtain private information on both foreign and American citizens. To ensure these tools are being used appropriately, we required the Inspector General of the Department of Justice to submit reports on the use of the two most far-reaching provisions -- Section 215, which allows searches for business records, and Section 505, which authorizes National Security Letters to collect information in national security investigations. The Inspector General determined that the FBI circumvented the laws governing the use of National Security Letters by issuing "exigent letters" in non-emergency circumstances, by failing to ensure that there were duly authorized investigations and by inaccurately representing that the FBI had requested subpoenas for the information when, in fact, it had not.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00160 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.035

As the Inspector General's first report makes clear, our concerns were well founded. The FBI's misuse of National Security Letters and "exigent letters" has been a gross invasion of privacy. The Administration's excuse of "fighting the war on terror" does not justify the violation of basic constitutional rights and civil liberties.

The lack of instruction and supervision within the FBI is unacceptable. The Inspector General found that that the FBI's "widespread and serious misuse" of these intrusive investigatory tools was the product of "mistakes, carelessness, confusion, sloppiness, lack of training, lack of adequate guidance and lack of adequate oversight." The FBI must take responsibility for these mistakes and work to correct them immediately. The American people deserve protection from such reckless and improper investigations and I look forward to working with my colleagues on the Judiciary Committee to end these abuses as soon as possible. No Administration is entitled to operate unchecked and unaccountable, with such blatant disregard for the rule of law.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00161 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.036

STATEMENT OF SENATOR PATRICK LEAHY,
CHAIRMAN, COMMITTEE ON THE JUDICIARY
HEARING ON FBI OVERSIGHT
MARCH 27, 2007

The Committee today continues its crucial oversight role of the Department of Justice with this hearing to examine the FBI's effectiveness in carrying out its domestic intelligence and law enforcement mission. I thank the FBI Director for appearing before us today. I look forward to hearing his views on the Bureau's problems and progress. I also thank the hard-working men and women of the FBI, who have been working long hours, day after day, week after week, year after year, to help keep our citizens and communities safe.

Almost six years after the September 11th attacks, it troubles all of us that the FBI has not yet lived up to its promise to be the world-class domestic intelligence agency that the American people expect and need it to be. This morning, we learned from a report in the *Washington Post* that the FBI has repeatedly submitted inaccurate information to the Foreign Intelligence Surveillance Court ("FISC") in its efforts to obtain secret warrants in terrorism and espionage cases -- severely undermining the Government's credibility in the eyes of the Chief Judge of that Court.

This failure compounds the serious concerns raised in recent months about the management and priorities of this Department of Justice. From the FBI's illegal and improper use of National Security Letters (NSLs), to the Bureau's failure to be accountable for and secure its own computers and weapons, to the politically motivated dismissal of eight of the Nation's U.S. Attorneys, there are growing concerns about the competence of the FBI and the independence of the Department of Justice. This pattern of abuse of authority and mismanagement causes me, and many others on both sides of the aisle, to wonder whether the FBI and Department of Justice have been faithful trustees of the great trust that the Congress and American people have placed in them to keep our Nation safe, while respecting the privacy rights and civil liberties of all Americans.

And it is more than just the FBI that deserves scrutiny for the abuses and lack of competence that have come to light just in recent weeks. Last year the Administration sought new powers in the PATRIOT Act to appoint U.S. Attorneys without Senate confirmation, and to more freely use National Security Letters. The Administration got these powers, and they have badly bungled both.

National Security Letters

One of my priorities in the first PATRIOT Act was to improve oversight and accountability. Former House Majority Leader Dick Armey and I insisted on, and succeeded, in adding sunset provisions to the PATRIOT Act, which is why Congress had to review and reauthorize several of the Act's most sweeping powers. In the recent

38189.037

reauthorization of the Act, one of my priorities – working especially with then-Chairman Specter -- was to retain sunset provisions and to supplement them with new "sunshine" provisions, to require the Justice Department to report to the Congress and to the American people on how several of the Act's powers are being used. The Inspector General's audit and report on National Security Letters was one of these new requirements we added to the law, and the troubling findings of that audit are why we are here today.

I am deeply disturbed by the Justice Department Inspector General's report finding widespread illegal and improper use of NSLs to obtain Americans' phone and financial records. The Inspector General found 22 separate instances where the FBI improperly abused NSLs in his office's review of just 77 FBI files. Not a single one of these violations had been reported by the FBI.

Even more troubling is that the violations the Inspector General uncovered are probably just the tip of the iceberg. When he appeared before Congress last week, Inspector General Glenn Fine testified that there could be thousands of additional violations among the tens of thousands of NSLs that the FBI is now using each year.

The Inspector General also found widespread use by the FBI of so-called "exigent letters." These letters, which are not authorized by any statute, were issued at least 739 times to obtain Americans' phone records when there was often no emergency and never a follow-up subpoena, as promised in the letters. Despite these extensive abuses, the top leadership at the FBI sat idly by for years, doing nothing to stop this practice. In fact, The Washington Post recently reported that FBI counterterrorism officials continued to use the "exigent letters," even though FBI lawyers and managers expressed reservations about this practice as early as 2004.

These abuses are unacceptable. I look forward to Director Mueller's explanation of how they occurred and what the FBI is doing -- now that our oversight required a public report of these failures – to ensure that these abuses and violations never happen again.

Lack of Accountability -- Lost Laptops and Weapons

The pattern of incompetence and lack of accountability within the Department and at the Bureau is also on display with the FBI's treatment of its own equipment and weapons. Another recent report by the Justice Department's Inspector General found that the FBI cannot account for 160 laptop computers and an equal number of weapons that were lost or stolen over a three-and a-half year period. This finding comes four years after the Inspector General recommended that the FBI take steps to ensure the security of this equipment. Even more troubling, Inspector General Fine found that in many cases, the FBI could not even determine whether its lost or stolen computers contained classified or sensitive information, putting Bureau employees and other individuals at risk of becoming victims of identity theft and potentially compromising national security information.

38189.038

Counterterrorism and Sentinel

These reports make it clear that the FBI is still not as strong and as equipped as it must be to fulfill its counterterrorism mission. The FBI still lags far behind where it needs to be when it comes to the number of agents that it has who are proficient in Arabic.
Last month, the Office of Inspector General also found that the FBI did not accurately report its terrorism-related convictions and other terrorism statistics in 2004.

In addition, years after 9/11, the FBI still does not have the information technology that it needs to function efficiently in the Information Age. Inspector General Fine found that the database that the FBI used to track NSLs malfunctioned, making it impossible to keep track of these letters. And, just recently, we learned a familiar piece of news regarding the FBI's project to upgrade its computer system. Apparently there will be delays in the deployment of Phase I of the FBI's Sentinel computer upgrade program – possibly jeopardizing the schedule for this much-needed computer system. This latest setback is one of a string of costly delays in the FBI's efforts to upgrade its computers. The Sentinel project was supposed to be different. Sentinel was launched after watching the FBI waste five years and millions of taxpayer dollars on the failed Trilogy program. I remain seriously concerned about this project.

Conclusion

The FBI is again at a crossroads. Because of these, and other, shortcomings, some are calling on Congress to take away the FBI's domestic intelligence functions altogether and to create a separate domestic intelligence agency like Britain's MI5. Last week the leading Republican on this oversight Committee questioned whether Director Mueller is up to the job.

Acknowledging shortcomings is well and good -- and Director Mueller now says that he takes responsibility for the egregious violations that occurred regarding the handling of NSLs, as he should. But the Bureau -- and the Department as a whole -- must also learn from its mistakes if progress is to be made. The time has come for demonstrable progress by the Bureau on a learning curve that has gone on and on for far too long.

Much work remains to be done and this Committee intends to fulfill its obligation to the American people to carefully examine all of these issues. Not having answers to our questions from our last oversight hearing three months ago is not the way to make progress. As I said to Director Mueller in my letter to him several weeks ago, I want the FBI to be the best that it can be, and oversight is part of the formula that is needed for achieving the improvements we need.

# # # # #

38189.039

PATRICK J. LEAHY, VERMONT, CHAIRMAN

EDWARD M. KENNEDY, MASSACHUSETTS
JOSEPH R. BIDEN, JR., DELAWARE
HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
RUSSELL D. FEINGOLD, WISCONSIN
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
BENJAMIN L. CARDIN, MARYLAND
SHELDON WHITEHOUSE, RHODE ISLAND

ARLEN SPECTER, PENNSYLVANIA
ORRIN G. HATCH, UTAH
CHARLES E. GRASSLEY, IOWA
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
SAM BROWNBACK, KANSAS
TOM COBURN, OKLAHOMA

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

March 6, 2007

Honorable Robert Mueller
Director
Federal Bureau of Investigation
U.S. Department of Justice
Washington, D.C. 20535-0001

Dear Director Mueller:

I am sorry to hear that your knee operation is still given you problems. I hope that you feel better soon and are better than new in no time.

I saw some of the extensive press conference you conducted this past week on unsolved civil rights cases from decades ago. Congressman Lewis is leading the effort to create a unit at the Department of Justice in connection with such matters. I have cosponsored Senator Dodd's Senate companion bill and expect we will enact it this year.

I have rescheduled the FBI oversight hearing from March 14 to March 27 to accommodate your recovery. Please provide a copy of your written testimony and curriculum vitae for distribution to Members of the Committee at least 24 hours before the hearing is scheduled to begin. Please send an electronic copy of your testimony and a short biography via email to LGW@judiciary-dem.Senate.gov. We will need 75 hard copies of the written testimony to distribute to Members, the press and the public. We would appreciate your providing those hard copies 24 hours in advance of the hearing, as well. Please send the hard copies of your testimony and curriculum vitae to the attention of Leila George-Wheeler, Senate Committee on the Judiciary, 224 Dirksen Senate Office Building, Washington, D.C. 20510.

I trust that by March 14 we will finally have answers to the written questions propounded in connection with your last appearance before the Committee early last December. The recent letter from your staff saying that you provided your responses to the Department of Justice does not substitute for timely answers the Committee's questions. March 14 will be more than three months since the questions were propounded. Although that would cut in half the six-month delay we experienced after your previous appearance before the Committee and be a step in the right direction, we need to do better.

Honorable Director Mueller
March 6, 2007
Page 2 of 2

You would not tolerate this kind of response time in an FBI investigation where months go by without answers and by the time responses are provided they are outdated or superseded by events. That is not conducive to effective oversight.

I want the FBI to be the best it can be. I believe effective oversight can contribute to its improvement.

Sincerely,

PATRICK LEAHY
Chairman

I know justice can be frustrating but they are not helping you with this delay

Statement of
Robert S. Mueller, III
Director
Federal Bureau of Investigation
Before the
United States Senate
Committee on the Judiciary

March 27, 2007

Good morning Mr. Chairman, Senator Specter, and Members of the Committee. Thank you for opportunity to testify before you this morning. Last week, the Committee heard testimony from Glenn Fine, the Inspector General of the Department of Justice regarding a recent report issued by his office on the FBI's use of national security letters, or NSLs. The Inspector General and his staff conducted a thorough and fair review of this authority and the Congress is to be commended for requiring that this review be conducted. As you heard from the Inspector General, he did not find any deliberate or intentional misuse of the national security letter authorities, Attorney General Guidelines or FBI policy. Nevertheless, the review by the Office of Inspector General (OIG) identified several areas of inadequate auditing and oversight of these vital investigative tools, as well as processes that were inappropriate. Although not intentionally, we fell short in our obligations to report to Congress on the frequency with which we use this tool and in the internal controls we put into place to make sure that it was used only in accordance with the letter of the law. I take responsibility for those shortcomings and for

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00167 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.042

shortcomings and for taking the steps to ensure that they do not happen again. The OIG report made ten recommendations designed to provide both the necessary controls over the issuance of NSLs and the creation and maintenance of accurate records. I fully support each recommendation and concur with the Inspector General that, when implemented, these reforms will ensure full compliance with both the letter and the spirit of the authorities entrusted to the Bureau by the Congress and the American people.

National Security Letters generally permit us to obtain the same sort of documents from third party businesses that prosecutors and agents obtain in criminal investigations with grand jury subpoenas. Unlike grand jury subpoenas, however, NSL authority comes through several distinct statutes and they have specific rules that accompany them. NSLs have been instrumental in breaking up cells like the "Portland Seven," the "Lackawanna Six," and the "Northern Virginia Jihad." Through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone and e-mail linkages that resulted in further investigation and arrests, and arrested suspicious associates with deadly weapons and explosives.

National Security Letter Authorities

The NSL authority used most frequently by the FBI is that provided by the Electronic Communications Privacy Act (ECPA). Through an ECPA NSL, the FBI can obtain subscriber information for telephones and electronic communications and can obtain toll billing information and electronic communication transaction records. Significantly, the FBI cannot obtain the content of communications through an ECPA NSL. Although the exact numbers of ECPA NSLs remains

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00168 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.043

classified, it is the most common NSL authority used.

Pursuant to the Right to Financial Privacy Act (RFPA), the FBI also has the authority to issue NSLs for financial records from a financial institution. RFPA NSLs are used commonly in connection with investigations of potential terror financing.

Pursuant to the Fair Credit Reporting Act, the FBI has the authority to issue three different, but related, types of NSLs to credit reporting agencies: an NSL pursuant to 15 U.S.C. 1681u(a) for the names of financial institutions with which the subject has or has had an account; an NSL pursuant to 15 U.S.C. 1681u(b) for consumer identifying information (name, address, former addresses, employment and former employment); an NSL pursuant to 15 U.S.C. 1681v for a full credit report. Of all the FBI"s NSL authorities, only the last of the FCRA authorities is restricted to use only in international terrorism cases.

Finally, the FBI has the authority to issue NSLs pursuant to the National Security Act in the course of investigations of improper disclosure of classified information by government employees.

For the first 3 types of NSLs (ECPA, RFPA, FCRA) the NSL must include a certification by an authorized FBI employee that the material is being sought for an authorized national security investigation. That certification is slightly different in the case of a FCRA NSL for a full credit report, where the certification required is that the information is relevant to an international terrorism investigation.

The authority to issue an NSL lies at a senior level within the FBI. An NSL can be issued only by an official who ranks not lower than Special Agent in Charge or Deputy Assistant Director. All such officials are career government employees who are members of the Senior Executive Service.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00169 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.044

Procedurally, an agent or analyst seeking an NSL must prepare a document (an electronic communication or EC) in which the employee lays out the factual predicate for the request. The factual recitation must be sufficiently detailed so that the approving official can determine that the material sought is relevant to an investigation. Additionally, it needs to provide sufficient information concerning the underlying investigation so that reviewing officials can confirm that the investigation is adequately predicated and not based solely on the exercise of First Amendment rights. Finally, the EC includes a "lead" to the Office of the General Counsel (OGC) for purposes of Congressional reporting.

The OIG Report

As directed by Congress, we endeavored to declassify as much information as possible concerning our use of NSLs in order to allow the maximum amount of public awareness of the extent of our use of the NSL tool consistent with national security concerns. To that end, for the first time the public has a sense of the frequency with which the FBI makes requests for data with national security letters. In the period covered by the report, the number of NSL requests has ranged from approximately 40,000 to 60,000 per year and we have requested information on less than 20,000 persons per year. For a variety of reasons that will be discussed below, those numbers are not exact. Nevertheless, they, for the first time, allow the public to get some sense of the order of magnitude of these requests; there are a substantial number of requests, but we are not collecting information on hundreds of thousands of Americans.

There are three findings by the OIG that are particularly disturbing, and it is those three findings that I wish to address this morning: (1) inaccurate reporting to Congress of various data points we are

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00170 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.045

obligated to report relative to NSLs; (2) the use of so-called exigent letters that circumvented the procedures required by ECPA; and (3) known violations (both previously self-reported by FBI and not previously reported) of law and policy with regard to usage of NSLs.

Congressional Reporting

A finding of the report that particularly distresses me is the section that addresses the inaccuracies of the numbers we report to Congress. The process for tabulating NSLs simply did not keep up with the volume. Although we came to that realization prior to the OIG report and are working on a technological solution, that realization came later than it should have.

The tracking of NSLs for Congressional reporting purposes resides in a standalone Access database. This database is referred to in the OIG report as the OGC database. While the OGC database was a major technological step forward from 3 x 5 index cards once used to track NSLs, it is not an acceptable system given the significant increase in use of NSLs since 9/11. First and foremost, the OGC database is not electronically connected to ACS, the system from which we derive the data. Instead, there is a manual interface between ACS and the OGC database. An OGC employee is responsible for taking every NSL lead that is sent to OGC and manually entering the pertinent information into the OGC database. Nearly a dozen fields must be manually entered, including the file number of the case in which the NSL was issued (typically 15 digits and alphanumeric identifiers).

Approximately a year ago, we recognized that our technology was inadequate and began developing an automated system to improve our ability to collect this data. The system, in addition to improving data collection, will automatically prevent many of the errors in NSLs that we will discuss

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00171 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.046

today. We are building an NSL system to function as a workflow tool that will automate much of the work that is associated with preparing NSLs and the associated paperwork. The NSL system is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can automatically ensure that certain legal and administrative requirements are met and that required reporting data is accurately collected. For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system will be able to verify the status of that file to ensure that it is still open and current (e.g. request date is within six months of the opening or an extension has been filed for the investigation) and ensure that NSLs are not being requested out of control or administrative files. The system will require the user to separately identify the target of the investigative file and the person whose records are being obtained through the requested NSL, if different. This will allow the FBI to accurately count the number of different persons about whom we gather data through NSLs. The system will also require that specific data elements be entered before the process can continue, such as requiring that the target's status as a United States Person or non-United States Person be entered. The system will not permit requests containing logically inconsistent answers to proceed.

The NSL system is being designed so that the FBI employee requesting an NSL will enter data only once. For example, an agent or analyst who wishes to get telephone toll billing records will only have to prompt the system that he is seeking an ECPA NSL for toll records and type the telephone number once. The system will then automatically populate the appropriate fields in the NSL and the authorizing EC. The system will then generate both the NSL and the authorizing EC for signature,

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00172 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.047

thereby ensuring that the two documents match exactly and minimizing the opportunity for transcription errors that give rise to unauthorized collections that must be reported to the Intelligence Oversight Board (IOB). Agents and analysts will still be required to provide the narrative necessary to explain why the NSL is being sought, the factual basis for making a determination that the information is relevant to an appropriately predicated national security investigation, and the factual basis for a determination whether the NSL should include a non-disclosure provision. In addition, this system will have a comprehensive reporting capability.

We began working with developers on the NSL system in February 2006 and we are optimistic that we will be able to pilot it this summer and roll it out to all field offices by the end of the year. At that point, I will be confident the data we provide to Congress in future reports is as accurate as humanly possible.

In the meantime, we are taking several steps to correct the numbers we have previously reported. First, we are making data corrections in our database. Through a computer program, we have identified all entries that must be erroneous because there is an apparent error in the entry (e.g., there are more NSLs reported than requests; the date shows a year that is impossible (203)). We are manually reviewing those entries and making corrections. We have also started a random sampling of ten percent of the total entries in the OGC database which contains approximately 64,000 entries. Those entries will be manually checked against ACS. We will determine whether there is a significant difference between the entries in our database and the actual information in ACS. To the extent there is a difference, that will be the factor that will be used to correct our prior reporting. While not yielding an exact count, we believe that to be a statistically appropriate way of correcting prior reporting. We

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00173 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.048

have discussed this methodology with the OIG and will offer it the opportunity to review our work. We are striving to have corrected reports to Congress as soon as possible.

As with the other shortcomings identified by the OIG, there was no finding of an intent to deceive Congress concerning our use of NSLs. In fact, as noted, we identified deficiencies in our system for generating data prior to the initiation of the OIG's review and flagged the issue for Congress almost one year ago. While we do not know the extent of the inaccuracies in past reporting, we are confident that the numbers will not change by an order of magnitude.

Exigent Letters

The next significant finding of the OIG involved the use within one unit at Headquarters of so-called "exigent letters." These letters, which numbered in excess of 700, were provided to telephone companies with requests for toll billing information regarding telephone numbers. All of the letters stated that there were exigent circumstances. Many of the letters stated that federal grand jury subpoenas had been requested for the records even though in fact no such request for grand jury subpoenas had been made, while others promised future national security letters. From an audit and internal control perspective, the FBI did not document the nature of the emergency circumstances that led it to ask for toll records in advance of proper legal process, did not keep copies of all of the exigent letters it provided to the telephone companies, and did not keep records showing that it had subsequently provided either the legal process promised or any other legal process. Further, based on interviews the OIG conducted, some employees indicated that there was not always any emergency relating to the documents that were sought.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00174 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.049

OGC has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided. As of late last week, there were still a small handful of telephone numbers that had not been satisfactorily tied to an authorized investigation. If we are unable to determine the investigation to which those telephone numbers relate, they will be removed from our database and destroyed.

The OIG rightfully objected to the FBI obtaining telephone records by providing a telephone carrier with a letter that states that a federal grand jury subpoena had been requested when that was untrue. It is unclear at this point why that happened. I have ordered a special inspection in order to better understand the full scope of internal control lapses.

We also concur with the OIG that it is inappropriate to obtain records on the basis of a purported emergency if, in fact, there is no emergency. We continue to believe, however, that providers had the right to rely on our representation that there was an emergency and that the "exigent letters" - had they been issued only when there was an exigent circumstance and had they correctly identified the legal process that would follow - would have been an appropriate tool to use.

In response to the obvious internal control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Any agent who needs to obtain ECPA-protected records on an emergency basis must now do so pursuant to 18 U.S.C. 2702. Section 2702(c)(4) permits a carrier to provide information regarding its customers to the government if the provider in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency. A request for

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00175 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.050

disclosure pursuant to that statute generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The letter request must also set out the basic facts of the emergency so that the provider can make some assessment whether it concurs that there is an emergency.

Intelligence Oversight Board Process

The OIG also examined misuse of NSLs that had been reported (and some that had not been reported) as part of the IOB process. As this committee knows, pursuant to Executive Order 12863 the President has an Intelligence Oversight Board that receives from the agencies in the intelligence community reports of intelligence activities that the agency believes may have been unlawful or contrary to Executive Order or Presidential Directive. This language is interpreted by the FBI and DOJ to mandate the reporting of any violation of a provision of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection if such provision is designed to ensure the protection of individual rights.

The FBI requires its employees to report any violations of law or policy about which they are aware. We encourage employees to err on the side of reporting so that we can be sure that all violations are appropriately reported. In terms of process, all potential violations are reported to OGC. Lawyers within OGC are responsible for "adjudicating" the violation - that is, determining whether the potential violation is an actual Intelligence Oversight Board violation. If it is, a report is made to the IOB, a copy is provided to DOJ and a copy is provided to the FBI's Inspection Division. If the violation involved intentional misconduct, the Inspection Division will determine whether the matter

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00176 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.051

should be referred to the Office of Professional Responsibility for discipline.

The OIG found that from 2003 through 2005, the FBI had self-reported 26 potential violations involving NSL authorities. Of the 26, OGC adjudicated 19 to be violations and reported them. The OIG agreed with each of those determinations. Of the 7 potential violations that OGC determined were not violations, the OIG agreed with all but one. As to the one determination about which we disagreed, upon re-review, the FBI concurred with the OIG that it was a violation that should have been reported and it has since been reported to the IOB. These 20 violations included: third party errors (4), NSLs issued when the authority for the investigation had lapsed (3), obtaining ECPA-protected records without any legal process (3) and obtaining a full credit report in a counterintelligence case (1).

The OIG also found, however, a number of potential IOBs in the files it examined that had not been reported to OGC for adjudication. The OIG examined 293 NSLs - a reasonably small sample. The sample was a judgmental sample and the size was chosen because the audit was extremely labor intensive. We do not suggest that the sample was not a fair sample (although it was not random), but only that it is questionable from a statistical standpoint to attempt to extrapolate from a very small sample to an entire population. Moreover, there was wide variation in the number of purported unreported violations from different field offices. The OIG found 8 potential violations that were unreported in files in both the Philadelphia and Chicago field offices, but only 2 unreported potential violations from files in New York and 4 from San Francisco. We are doing additional follow-up work, but the wide variance between field offices may be a function of the very small sample, or it may indicate that the percentages of potential errors detected are not constant across all field offices.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00177 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.052

Of the 293 NSLs the OIG examined, 22 (7%) were judged to have potential unreported IOB violations associated with them. Moreover, of those 22 NSLs, 10 - or almost 50% - were third party errors -- that is, the NSL recipient provided the FBI with information we did not seek. Only 12 of the NSLs examined - 4% - had mistakes that the OIG rightfully attributes to the FBI.

Examining the 12 potential errors that were rightfully attributed to the FBI reveals a continuum of seriousness relative to the potential impact on individual rights. Four (or just over 1% of the sample) were serious violations. Specifically, two of the violations involved obtaining full credit reports in counterintelligence investigations (which is not statutorily authorized), one involved issuing an NSL when authorization for the investigation to which it related had lapsed, and one involved issuing an NSL for information that was arguably content, and therefore not available pursuant to an NSL. (In the latter case, the ISP on which the NSL was served declined to produce the requested material so there was, in fact, no collection of information to which we were not entitled.) The balance of the 12 potential violations identified by the OIG do not, in our view, rise to the same level of seriousness as those 4. The remaining 8 involve errors that are best characterized as arising from a lack of attention to detail, and did not result in the FBI seeking or obtaining any information to which it was not entitled. Those 8 potential violations involved errors such as using the wrong certification language in an NSL (although the appropriate certification is not materially different) and having the NSL and the EC seeking the NSL not entirely consistent. We do not excuse such lack of attention to detail, but we do not believe that such mistakes result in or cause a risk to civil liberties.

In short, approximately 1% of the NSLs examined by the OIG had significant errors that were attributable to FBI actions and that had not been, but should have been, reported as potential IOB

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00178 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.053

violations.

While a 1% error rate is not huge, it is unacceptable, and we have taken steps to reduce that error rate. First, we are very concerned that of all the potential IOBs involving mistakes in NSLs attributable to the FBI (whether previously reported or not), 3 involved the same mistake: namely, issuing an NSL for a full credit report in a counterintelligence investigation. In order to ensure that this particular error is fully rectified, I have ordered all FBI field offices to examine all counterintelligence files in which Fair Credit Report NSLs have been issued since January 1, 2002 in order to ascertain whether the file contains a full credit report. If it does, the credit report must be removed from the file, sequestered with the field office's attorney, and a potential IOB violation must be reported to OGC. The results from that search are due to headquarters by mid-April 2007.

Additional Corrective Steps

Several other steps we have taken will, we believe, reduce the likelihood that the FBI will commit the other mistakes in the future. First, as indicated previously, the FBI is developing an automated system to prepare NSLs and their authorizing ECs. That system will reduce to zero mistakes such as having the wrong certification language or inconsistency between the NSL and the EC. It will also ensure that the investigative file out of which the NSL is being issued is open. Finally, it will ensure that an NSL for a full credit report cannot be issued out of a counterintelligence file.

Other changes to FBI policy have been made that we believe will facilitate better handling of IOBs and also reduce errors that lead to IOBs. First, last fall we provided comprehensive advice to the field regarding its responsibility towards information obtained as a result of third party errors. That guidance requires all such information to be sequestered and reported to OGC as a potential IOB. If

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00179 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.054

the "over collected" information is irrelevant to the investigation (e.g., the telephone company transposed a number and provided us records on the wrong telephone account), then it will be destroyed or returned. No such information should be entered into FBI databases. If the information is relevant to the investigation but simply not within the four corners of the NSL, then the information must be sequestered until a new NSL has been issued for the extra data. After the new NSL has been issued, the information can be entered into FBI databases.

Secondly, we have collected all the rules and policies on NSLs into one document which will be disseminated to the field. Those rules now mandate that, until the deployment of the automated NSL system, all NSLs and ECs be prepared from the exemplars that are provided on OGC's website. That should eliminate many of the mistakes identified by the OIG.

All of these rules will, of course, only reduce or eliminate errors if they are followed. The OIG's report has highlighted for us that there must be some sort of auditing function - above and beyond the IOB process - to systematically ensure that these rules, as well as others that govern our activities in national security investigations are followed. The FBI has historically been very good at establishing policy and setting rules, but we have not been as proactive as we should have been in establishing internal controls and auditing functions.

The full parameters of the compliance program have not been set, although these aspects have been: the Inspection Division with participation of DOJ's National Security Division and Privacy and Civil Liberties Office is in the process of a special inspection of NSL usage in all 56 field offices and headquarters. That inspection should uncover any other significant problems with our use of this tool but should also tell us whether there are variances between offices in terms of the numbers and types of

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00180 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.055

errors. The results of the inspection will then inform the program that the Attorney General announced of having teams of DOJ lawyers, FBI lawyers and the Inspection Division periodically audit field offices' use of NSLs. That process will begin in April and should result in at least 15 offices being audited this year. We are also considering other proactive compliance programs in order to develop a program that ensures, to the maximum extent possible, that the rules and policies designed to protect privacy and civil liberties are faithfully adhered to by all of our employees, that we promptly identify and correct any violations of law or policy, and that any information collected erroneously is removed from FBI databases and destroyed. In addition, a working group co-chaired by the Office of the Director of National Intelligence and the CPCLO has been convened to examine how NSL-derived information is used and retained by the FBI. The FBI and DOJ's National Security Division will have a representative on this working group. We welcome the Committee's input as we move forward on these initiatives.

Mr. Chairman, the FBI is acutely aware that we cannot protect against threats at the expense of civil liberties. We are judged not just by our ability to defend the nation from terrorist attacks but also our commitment to defend the rights and freedoms we all enjoy. In light of the Inspector General's findings, we are committed to demonstrating to this Committee, to the Congress, and to the American people that we will correct these deficiencies and utilize the critical tools Congress has provided us consistent with the privacy protections and civil liberties that we are sworn to uphold.

I appreciate the opportunity to appear before the Committee and look forward to answering your questions. Thank you.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00181 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.056

FBI Provided Inaccurate Data for Surveillance Warrants

By John Solomon
Washington Post Staff Writer
Tuesday, March 27, 2007; A05

FBI agents repeatedly provided inaccurate information to win secret court approval of surveillance warrants in terrorism and espionage cases, prompting officials to tighten controls on the way the bureau uses that powerful anti-terrorism tool, according to Justice Department and FBI officials.

The errors were pervasive enough that the chief judge of the Foreign Intelligence Surveillance Court, Colleen Kollar-Kotelly, wrote the Justice Department in December 2005 to complain. She raised the possibility of requiring counterterrorism agents to swear in her courtroom that the information they were providing was accurate, a procedure that could have slowed such investigations drastically.

A internal FBI review in early 2006 of some of the more than 2,000 surveillance warrants the bureau obtains each year confirmed that dozens of inaccuracies had been provided to the court. The errors ranged from innocuous lapses, such as the wrong description of family relationships, to more serious problems, such as citing information from informants who were no longer active, officials said.

The FBI contends that none of the mistakes were serious enough to reverse judges' findings that there was probable cause to issue a surveillance warrant. But officials said the errors were significant enough to prompt reforms bureau-wide.

"It is clear to everybody this is a serious matter. This is something that has to happen quickly. We have to have the confidence of the American people that we are using these tools appropriately," said Kenneth Wainstein, the Justice Department's new assistant attorney general for national security.

The department's acknowledgment of the problems with the FISA court applications comes nearly two weeks after a blistering inspector general's report revealed widespread violations of the use of "national security" and "exigent circumstances" letters, which allow FBI agents to collect phone, e-mail and Internet records from telecommunications companies without review by a judge. The problems included failing to document relevant evidence, claiming emergencies that did not exist and failing to show that phone records requests were connected to authorized investigations.

In the use of both national security letters and the FISA warrant applications, officials acknowledged that the problems resulted from agents' haste or sloppiness -- or both -- and that there was inadequate supervision.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00182 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.057

"We've oftentimes been better at setting the rules than we have been at establishing the internal controls and audits necessary to enforce them," FBI Assistant Director John Miller said.

FBI Director Robert S. Mueller III is scheduled to appear before the Senate Judiciary Committee today to answer questions about the use of national security letters. Congress will receive its annual report on FISA warrants next month.

Experts said Congress, the courts and the Justice Department share the blame for not conducting more aggressive oversight of FBI agents.

"It is a little too easy to blame the FBI, because the FBI gets away with this stuff when the other institutions of government fail to do their jobs," said Marc Rotenberg, president of the Electronic Privacy Information Center, which monitors civil liberties issues.

Records show that the FISA court approves almost every application for the warrants, which give agents broad powers to electronically monitor and surveil people who they allege are connected to terrorism or espionage cases. The number of requests rose from 886 in 1999 to 2,074 in 2005. The court did not reject a single application in 2005 but "modified" 61, according to a Justice Department report to Congress.

Senior Justice officials said they have begun a comprehensive review of all terrorism-fighting tools and their compliance with the law. That will be followed by regular audits and training to ensure that agents do not lapse into shortcuts that can cause unintended legal consequences.

Wainstein noted that before his division was created last year, the Justice Department could not systematically check FBI compliance with rules in all types of national security investigations. He acknowledged, for instance, that the department was told of 26 potential violations that the FBI had disclosed in its use of national security letters but did not focus on them.

Earlier this year, President Bush agreed to allow the FISA court to review surveillance requests from the National Security Agency after a battle with civil liberties groups and some lawmakers over the legality of that agency's spying effort, in which some suspects were overseas.

Last year's problems involving the FISA court, however, involved the issuance of secret warrants that authorized FBI agents to conduct surveillance inside the United States.

Shortly before the Sept. 11, 2001, attacks, the FISA court complained that there were inaccuracies in 75 warrants that the court had approved going back several years. The FBI responded by instituting new policies to better ensure that the information agents provided in warrant applications was accurate and could be verified if questioned.

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00183 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.058

But audits conducted beginning in 2003 showed an increasing number of errors and corrections in applications. On Dec. 12, 2005, the court sent a letter of complaint that raised the idea of agents being compelled to swear to the accuracy of information.

Justice and the FBI are reviewing about 10 percent of the 60,000 ongoing terrorism investigation files in search of problems. "We are learning to live in a different environment, and now we are aware and working on problems, and I think we are creating a lot of fixes," said Jane Horvath, the Justice Department's first chief privacy and civil liberties officer.

FBI officials said they expect the audit of national security letters for 2006 to show the same problems as those identified in the current audit, which covered 2003 through 2005.

"You are never going to be at a zero error rate because this is a human endeavor," Wainstein said. "Therefore it is subject to error on occasion. But we're going to do everything we can to minimize them."

VerDate Nov 24 2008 09:28 Oct 06, 2009 Jkt 038189 PO 00000 Frm 00184 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\38189.TXT SJUD1 PsN: CMORC

38189.059