AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 108–804

FBI OVERSIGHT: TERRORISM AND OTHER TOPICS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MAY 20, 2004

Serial No. J–108–77

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

20–331 PDF WASHINGTON : 2005

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

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
LARRY E. CRAIG, Idaho
SAXBY CHAMBLISS, Georgia
JOHN CORNYN, Texas

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
JOHN EDWARDS, North Carolina

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

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cornyn, Hon. John, a U.S. Senator from the State of Texas	35
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois	44
Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin	29
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa, prepared statement	237
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	4
prepared statement	239
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	2
prepared statement	242
Schumer, Hon. Charles E., a U.S. Senator from the State of New York	38
prepared statement and attachments	258
Sessions, Hon. Jeff, a U.S. Senator from the State of Alabama	41

WITNESSES

Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C.	6

QUESTIONS AND ANSWERS

Responses of Robert S. Mueller to questions submitted by Senator Hatch	49
Responses of Robert S. Mueller to questions submitted by Senator Grassley	51
Responses of Robert S. Mueller to questions submitted by Senator Leahy	56
Responses of Robert S. Mueller to questions submitted by Senator Kennedy	119
Responses of Robert S. Mueller to questions submitted by Senator Feinstein	131
Responses of Robert S. Mueller to questions submitted by Senator Feingold	186
Responses of Robert S. Mueller to questions submitted by Senator Durbin	198

SUBMISSIONS FOR THE RECORD

Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement	250

FBI OVERSIGHT: TERRORISM AND OTHER TOPICS

THURSDAY, MAY 20, 2004

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

The Committee met, pursuant to notice, at 10:40 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senators Hatch, Grassley, Specter, Kyl, DeWine, Sessions, Craig, Cornyn, Leahy, Kohl, Feinstein, Feingold, Schumer and Durbin.

Chairman HATCH. We have got eight here. All we need is two more and we can finish this markup in a very short period of time. If and when the Director arrives, we will start with him until we get ten and I will interrupt to finish whatever we can on the markup and then go back to the Director. That way, we will get at least the minimum amount of work done that we have to get done today.

So if the Director is available, let's get him in here.

Welcome, Mr. Director. We have got nine here. As soon as we get ten, we will interrupt whatever we are doing and do the minimum that we can on the markup today. For instance, I would like to get Jonathan W. Dudas out, and we have got a couple of other bills that I think we can report, some of these S. Res. bills.

I will be very brief because, as Senators Leahy and Schumer have been requesting, we want the Committee to be able to hear from Director Mueller this morning. After Senator Leahy makes his opening statement or whatever he cares to make, I want to consider the nomination of Jon Dudas as soon as we get ten here to serve as Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office. As I understand it, there is no objection to him, but if there is, we will meet it at that time.

I also understand that we can move three commemoratives, two relating to World War II veterans and a third recognizing the *Brown* v. *Board of Education* decision, which we ought to all recognize. I also move that we can move S. 1933, the ENFORCE Act. We have come a long way on that.

So with that, I will turn to Senator Leahy for any comments he cares to make at this point.

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

Senator LEAHY. Mr. Chairman, thank you. I would note that the agenda does not have the Innocence Protection Act, even though you and I and Chairman Sensenbrenner and others made a commitment to the country, to the victims, to others, that we would move that bill.

I know that Chairman Sensenbrenner moved the bill, and he moved it in a conservative, Republican-controlled House with an overwhelming vote. We should try doing the same here. We have all had to make compromises on it. We have made commitments. He has fulfilled his promise and it is time for us to fulfill ours.

I am glad we are starting with the Director. Last time, we left him cooling his heels for an hour or two. I think that wasted his time and ours because, our oversight should be the most important thing we do up here. When it comes to the Justice Department, we don't do a great deal.

The cicadas come by every 17 years and that seems to be about the amount of time that passes between visits to us by the Attorney General. However, Director, I am glad you are here. I don't want the rhythm of this Committee to be connected to the 17-year rhythm of the cicadas.

I have been supportive of your efforts to more effectively concentrate the FBI's resources on the threats and challenges we face today. At the time of your nomination, I was the Chairman of the Committee and I worked hard to clear the path before you. I have done what I can since then to help you reform and refocus the Bureau.

When I have concerns, as you know, I pick up the phone and I share them with you privately; you don't read about them first in the paper. I very much wanted you to succeed when you began as Director, and I want you to succeed now. That is why I am going to raise several very serious questions.

We have all seen the photos from Abu Ghraib. Torture is a crime. It is a crime under the Convention Against Torture, to which we are a party. It is a crime under our laws. It undermines our National security. For months, the administration received warnings that this had been going on. I was one of the ones who wrote to them and warned them about it. Very little was done until the press came forward with the photographs. We were assured that things were fine. We were given self-serving reassuring statements that turned out to be false.

We read in one article about an Iraqi prisoner who said that after 18 days of being hooded and handcuffed, naked, dowsed with water, threatened with rape and forced to sit in his own urine, he was ready to confess to anything. When his interrogators asked him about Osama bin Laden, he replied "I am Osama bin Laden, I am in disguise." He would have admitted to being anybody else we asked him about.

The press accounts from last week suggested that the FBI shied away from participating in or observing certain interrogations of terrorism suspects. At the same time, it is clear from the Berg case that the FBI is operating in Iraq. So we need more information about what the FBI is doing here.

We have been assured in the thousand days since September 11 that big changes are taking place at the FBI. In our oversight role, this Committee examines actions. We learned from the hearings on September 11 that there were very serious problems at the FBI. And we should note for the record what should be self-evident: you came in only a few days before September 11. These problems were there long before you arrived.

The 9/11 Commission dealt the FBI some of the worst criticism yet, saying that much of the FBI does not work. A lot of the debate will examine whether the FBI is the right agency for the job of handling domestic intelligence and counter-terrorism.

None of us question the professionalism of your agents. Many of them put their lives on the line everyday. But we worry that you have not solved some of your most basic problems. Your information technology systems are hopelessly out of date. The FBI is not much better off today than it was before 9/11, when the FBI was unable to do a computer search of its own investigative files to make critical links and connections.

By all accounts, the Trilogy solution has been a disaster. I know I had a concern when I went down there and saw the state of the computer systems at the FBI after we spent hundreds of millions of dollars. I suspect most small county sheriffs' departments have better computer systems. We have put $500 or $600 million into improvements and the FBI system has to perform better than it does.

I could spend the whole session talking about the foreign translation program at the FBI. 41,000 hours in backlogged materials needed to be translated. How do you monitor the unprecedented 1,727 new FISA wiretaps calling on your resources? I asked in March of this year for the Chairman to have a full hearing on this, but we have yet to hear about that.

We want to hear from the Attorney General. You know, I find it amazing that on some of the things that the FBI and Justice Department are supposed to be doing, we hear from General Sanchez and General Abizaid earlier than we hear from the AG.

So these are my concerns. Regarding the FBI's computer system, I will mention one more thing: after 9/11, we saw people listening on a phone, writing down notes, handing them to somebody to rewrite and then handing them on again to somebody else to stick in the file; we saw an inability for agents to even e-mail the photographs of the people for which we are looking. My 12-year-old neighbor is in better shape.

But that is what you inherited; that is what you inherited the day you arrived. You were there only a few days before 9/11. Yet after hundreds and hundreds of millions of dollars later, I still wonder whether the computer systems are in the 21st century.

I have a lot more questions, Mr. Chairman, but I don't want to hold you up.

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

Chairman HATCH. We will provide time for that.

We have ten here, so I would like to at least get the minimal things done that we can.

[Whereupon, at 10:49 a.m., the Committee adjourned, to convene immediately in executive session. The Committee then reconvened at 10:51 a.m.]

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

Chairman HATCH. Now, if I can, I am going to make my opening remarks here this morning on the FBI Director.

Today, we are conducting an oversight hearing on the FBI's efforts to combat terrorism, as well as any other issues that my colleagues care to bring up.

We are going to have to have order.

I would like to welcome FBI Director Robert Mueller, who will testify before us today. I enjoyed our meeting earlier this month and I thought it was very productive. As many of you know, Director Mueller started his job one week prior to 9/11. And at that time, although the FBI was the subject of intense criticism and media coverage, Director Mueller was undaunted and took the job head-on. Over the last 3 years, I think he has accepted the challenge of transforming the FBI and has made every effort to help usher the FBI into the 21st century.

The challenges that he has undertaken are ambitious and, of course, cannot be completed overnight. In an agency that has 56 field offices, over 400 satellite offices, 52 overseas offices, and employs over 28,000 people, it is impossible to know what is going on in every place at every moment. Yet, Director Mueller had made it his business to find out where the trouble spots are and to take every measure to resolve problems, investigate any misconduct, and to seek outside expertise, when necessary, to address these issues.

The FBI's number one priority since 9/11 has been to protect the American people from another terrorist attack. In the subsequent 2 years and 8 months, the FBI has succeeded in that goal. Since September 11, 2001, more than 3,000 Al Qaeda leaders and foot soldiers have been taken into custody around the globe. Nearly 200 suspected terrorist associates have been charged with crimes in the United States, and as many as 100 terrorist attacks or plots have been broken up worldwide.

As we all know, before September 2001 we had communications challenges between the law enforcement community and the intelligence community. Sections 203 and 218 of the USA PATRIOT Act, which are due to expire on December 31, 2005, have been instrumental in breaking down the artificial wall of non-communication between the intelligence community and the law enforcement community.

By facilitating and encouraging increased communication among Federal agencies, the USA PATRIOT Act has paved the way for many of the coordination initiatives that Director Mueller has undertaken. Perhaps the greatest consequence of the tearing down of the wall is that it has set the stage for a new culture of cooperation within the Government.

Before 9/11, Federal, State and local agencies tended to operate individually. It takes time to change long-held cultural mores and to ensure that everyone is sharing information as they should. But

Director Mueller has taken several key steps in the right direction. Today, the FBI and the CIA are integrated at virtually every level of operations. Under Director Mueller's leadership, the FBI created the National Joint Terrorism Task Force, which works with the FBI's newly created Office of Intelligence to coordinate interagency intelligence-gathering activities and to act as a liaison between FBI headquarters and local JTTFs.

The FBI is also involved in the Terrorist Threat Integration Center, which was established last May at the direction of President Bush. It coordinates strategic analysis of threats based upon intelligence from the various agencies. In addition to all this, the FBI sends out weekly intelligence bulletins to over 1,700 law enforcement agencies and 60 Federal agencies. So I am looking forward to hearing more about these areas during this hearing.

These impressive accomplishments notwithstanding, the FBI still faces some very serious challenges. Let me start by commending Director Mueller for taking on the herculean task of modernizing the information technology systems at the FBI, a project which we all know as Trilogy. It is not an easy task to update both local and wide-area networks, and to install 30,000 new desktop computers. But you have accomplished that and I want to congratulate you for having done so.

On another note, I know that the FBI, like most Federal agencies, is facing the challenge of finding qualified linguists. While the demand for linguists in various dialects—Arabic, Farsi, Pashto, Urdu and other Asian and Middle Eastern languages—continues to be in high demand, I am heartened to hear that the FBI has added nearly 700 translators since September 2001.

I am reassured that the FBI has exacting standards, that 65 percent of its linguist applicants are screened out by a series of qualification tests, and that the FBI has quality control measures in place to ensure that the translations are accurate and complete.

Although I recognize that the FBI needs to hire more translators to meet their growing demand, I appreciate that you, Director Mueller, have adopted an aggressive recruitment strategy, advertising in both foreign-language and mainstream media, and targeting foreign language departments at American universities, military outplacement posts and local ethnic communities. I also appreciate that you have prioritized tasks so that the most significant counter-intelligence assignments are done first, often within 12 hours. I look forward to hearing more on this issue.

In the interest of brevity, I will submit the rest of my remarks for the record.

[The prepared statement of Chairman Hatch appears as a submission for the record.]

Chairman HATCH. Director Mueller, we will turn to Senator Leahy for a point and then we will turn to you for any comments you care to make.

Senator LEAHY. You know, there is so much good that has happened at the FBI under Director Mueller's tenure, but there is so much left to be done. There are two phases of Trilogy, as you mentioned, that were completed, I think, in April. So FBI agents can actually send e-mails to each other. This is not a thrilling accomplishment in this age. I have got a 6-year-old grandson who sends

me e-mails. This is not something that we should really say is a great accomplishment that FBI agents can e-mail each other, $500 to $600 million later.

The automated case system, the same system that was part of the equation of intelligence and law enforcement failure in 2001, is still the primary IT tool for agents. We are told that a virtual case file would mean the end of agency reliance on paper files which seem to get lost, and so on. We should take a look at the May 2004 report of the National Academy of Sciences which says that this virtual case file is not designed to, and it will not meet the FBI's counter-terrorism and counter-intelligence needs. This is a big agency, and I realize that there are areas of security that are needed, but this is too slow.

Thank you, Mr. Chairman.

Chairman HATCH. Thank you.

Let's hear what Director Mueller has to say.

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

Mr. MUELLER. Good morning. Thank you, Mr. Chairman, and also thank you, Senator Leahy, and thank you, members of the Committee for having me here today and giving me an opportunity to update you on what I believe is substantial progress we have made in the counter-terrorism and the intelligence arenas, as well as to advise the Committee on the effectiveness of the USA PATRIOT Act in the war on terror.

Before I do begin, however, I would like to acknowledge that none of our successes over the past two-and-a-half years would have been possible without the extraordinary efforts of our partners in State, local and municipal law enforcement, as well as our counterparts from around the world.

In addition, the Muslim–American, the Iraqi–American and the Arab–American communities have contributed substantially to any success that we will have had in the war on terror in the United States. And on behalf of the FBI, I would like to thank these communities for their assistance, as well as their ongoing commitment to preventing acts of terrorism. The country owes them a debt of gratitude.

Mr. Chairman, I would first like to acknowledge that the progress that the FBI has made in reforming our counter-terrorism and intelligence programs is due in no small part to the enactment of the USA PATRIOT Act. For over two-and-a-half years, the PATRIOT Act has proved extraordinarily beneficial in the war on terror and it has changed the way we in the FBI, as well as we in the intelligence community do our work.

Many of our counter-terrorism successes are the direct result of a number of PATRIOT Act provisions, some of which are scheduled to sunset at the end of next year. I do believe it is vital to our National security to keep each of these provisions intact. Without them, the FBI could be forced back into pre–September 11 practices, attempting to fight the war on terror with one hand tied behind our back.

Let me give you several examples that illustrate the importance of the PATRIOT Act to our counter-terrorism and our counter-intelligence efforts. First and foremost, the PATRIOT Act, along with the revision of the Attorney General's investigative guidelines and the 2002 decision of the foreign intelligence surveillance court, tore down the wall that stood between the intelligence officers of the United States and the criminal investigators who would be responding to the same terrorist threats.

Prior to September 11, if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case. And as important, if not more important, the opposite was also true that the information could not be shared from an intelligence investigation to a criminal investigation.

This increased ability to share information has disrupted terrorist operations in their early stages, such as the Portland 7 cell, and has led to numerous arrests, prosecutions and convictions in terrorist cases. Because the FBI can now share information freely with the CIA, with the NSA and with a host of other Federal, State, local and international partners, our resources are used more effectively, our investigations are conducted more efficiently, and American is immeasurably safer as a result. We just cannot afford to go back to the days when agents and prosecutors were afraid to share information.

The PATRIOT Act also updated the law to match current technology. So we no longer have to fight a 21st century battle with antiquated weapons. Terrorists exploit modern technology such as the Internet and cell phones to conduct and to conceal their activities. The PATRIOT Act leveled the playing field, allowing investigators to adapt to these modern technologies.

Today, court-approved roving wiretaps allow investigators to conduct electronic surveillance on a particular suspect, not a particular telephone. This technique has long been used to investigate crimes such as drug-trafficking and racketeering. In any world in which it is standard operating procedure for terrorists to rapidly change locations and to switch cell phones to evade surveillance, terrorism investigators must have access to the same tools.

Today, Federal judges have the authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigators. In the past, a court could only issue a search warrant for premises within the same judicial district, and yet our investigations of terrorist networks often span multiple districts. The PATRIOT Act also permits similar search warrants for electronic evidence such as e-mail.

In a final example, Mr. Chairman, the PATRIOT Act expanded our ability to pursue those who provide material support or resources to terrorist organizations. Terrorist networks rely on individuals for fundraising, procurement of weapons and explosives, training, logistics and recruiting. By criminalizing the actions of those who would provide, channel or direct resources to terrorists, the material support statutes provide an effective tool to intervene at the earliest possible stage of terrorist planning. This allows the FBI to arrest terrorists and their supporters before their deadly plans can be carried out.

As an example, the FBI's San Diego office recently conducted an investigation in which the subjects of the investigation negotiated with undercover law enforcement officials for the sale of heroin and hashish in exchange for Stinger anti-aircraft missiles. According to the subjects, the missiles were then to be sold to Al Qaeda.

Following a meeting with undercover agents in Hong Kong to finalize the purchase, the subjects were arrested by the Hong Kong police, working in conjunction with our legal attache overseas, and subsequently they were extradited to San Diego. Not only does this case highlight the importance of our overseas partnerships, but also the value of the material support provisions which allow prosecutors to charge subjects and to secure guilty pleas and convictions.

Mr. Chairman and members of the Committee, the importance of the PATRIOT Act as a valuable tool in the war against terrorism cannot be overstated. It is critical to our present and our future success. By responsibly using the statutes provided by Congress, we are better able to investigate and prevent terrorism and protect innocent lives, while at the same time protecting civil liberties.

Let me turn just for a minute to the progress the Bureau has made in strengthening and reforming our counter-terrorism and intelligence programs, doing so to support its number one priority, that of preventing another terrorist attack. Today, the FBI is taking full advantage of our dual role as both a law enforcement, as well as an intelligence agency. Let me give you a few examples of the progress we have made.

We have more than doubled the number of counter-terrorism agents, intelligence analysts and linguists. We expanded our Terrorism Financing Operations Program, which is dedicated to identifying, tracking and cutting off terrorist funds.

We created the Counterterrorism Watch at FBI Headquarters to receive threat information around the clock, to assess the credibility and urgency of the information, and to task appropriate FBI divisions to take action.

We expanded the number of Joint Terrorism Task Forces from 34 to 84 nationwide and established, as, Mr. Chairman, you pointed out, a National Joint Terrorism Task Force at FBI Headquarters. The task force is to serve as a conduit for threat information to the local Joint Terrorism Task Forces and to the 38 participating agencies, including, I might add, the Capitol Police.

We have created and refined new information-sharing systems such as the National Alert System that electronically links us with our State and local law enforcement partners. Lastly, we have sent approximately 275 FBI executives to the Kellogg School of Management at Northwestern University to receive training on executive leadership and strategic change within a large organization.

Recognizing that a strong, enterprise-wide intelligence program is critical to our success across all investigations, we have worked to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the FBI.

We established the Office of Intelligence, under the direction of Maureen Baginski, our Executive Assistant Director for Intelligence. Maureen, as most of you know, comes from a long career at the National Security Agency. The Office of Intelligence sets uni-

fied standards, policies and training for analysts, those analysts who examine intelligence and ensure that it is shared with our law enforcement and our intelligence partners. The Office of Intelligence has already provided over 2,600 intelligence reports and other documents for the President, the members of the community, and also for Congress.

We established a formal analyst training program and we are accelerating the hiring and training of analytical personnel and developing career paths for analysts that are commensurate with their importance to the mission of the FBI.

We developed and are in the process of executing concepts of operations governing all aspects of the intelligence process, from the identification of intelligence requirements to the methodology for intelligence assessment, to the drafting and formatting of intelligence products.

We established a requirements process to identify gaps in what we know, and to develop collection strategies to fill those gaps. We established Reports Officers positions and Field Intelligence Groups in every one of our field offices, whose members review investigative information not only for use in investigations in that field office, but also to disseminate that information throughout the FBI and among our law enforcement and intelligence community partners.

With these changes in place, the Intelligence Program is established and growing. We are now turning to the last structural step in our effort to build an intelligence capacity. In March we authorized new procedures governing the recruitment, the training, career paths and evaluation of our special agents, all of which are focused on developing intelligence expertise among our agent population.

The most far-reaching of these changes will be the new agent career path, which will guarantee that agents get experience in intelligence investigation and with intelligence processes. Under this plan new agents will spend an initial period of time familiarizing themselves with all aspects of the Bureau including intelligence collection and analysis, and then go on to specialize in counterterrorism, intelligence or another operational program.

The central part of this initiative will be an intelligence officer certification program that will be available to both analysts and agents, and that program will be modeled after and have the same training and experience requirements as the existing programs in the intelligence community.

All the progress that the FBI has made on its investigative fronts rests upon a strong foundation of information technology. Over the past two-and-a-half years the FBI has made a substantial effort to overhaul our information technology, and we, I believe, Mr. Chairman, and Senator Leahy, have made substantial progress.

Mr. Chairman, my prepared statement provides greater detail on the progress we have made in upgrading our information technology, and I will not go into the details here. I will say, however, that we have encountered problems, setbacks regarding the deployment of our infrastructure known as Full Site Capability that was due to come on line last October. The contractor indicated that the contractor would not be able to provide it by then. We went back

and renegotiated, and that Full Site capacity was completed on April 30th of this year.

We are on track to deliver elements of Virtual Case File capabilities by the end of this year. We are in negotiations with our contractor on finishing out that last part of the Trilogy Project.

And as, Senator Leahy, you have pointed out, the National Research Council of the National Academy of Sciences released a report reviewing our program, released it I believe last week or the week before. We commissioned this review as part of our ongoing efforts to improve our capabilities to assemble, analyze and disseminate investigative and operational data, both internally and externally, with other intelligence and law enforcement agencies. Many of the report's recommendations have already been implemented or are a work in progress, and my understanding is that the Council is looking at those portions of the recommendations that have been carried out and will be issuing a supplementary report.

I will again make the point that the FBI has repeatedly sought outside evaluation and advice throughout its IT modernization efforts, and we will continue to do so.

Let me conclude, if I might, Mr. Chairman, by saying that with the tools provided by the PATRIOT Act and with our counterterrorism, intelligence and information technology initiatives firmly in place, the FBI is moving steadily forward, always looking for ways to evolve and improve so that we remain several steps ahead of our enemies. We are looking at ways to assess and adjust our resource needs based on threats in order to ensure that we have the personnel and resources to fulfill our mission.

Mr. Chairman, let me finish by saying that I appreciate this Committee's continued support, and I appreciate the opportunity to be here this morning, and I am happy to answer any questions you might have.

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

Chairman HATCH. Thank you, Mr. Director. I am going to reserve my 10 minutes and turn to the Democratic Leader on the Committee first for questions. We are going to have one 10-minute round with every Senator given 10 minutes if he or she determines that is essential.

Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman. Again, I am glad that we are finally having this hearing. I read the press reports that make it very clear that the FBI is operating in Iraq. I think a lot of us on the Committee on both sides would like to know more about what the FBI is doing in Iraq. I will send you some written questions which will be basically this: How many agents do we have in Iraq? How long have they been there? What is their mission?

The reason I do this, because the Assistant Attorney General for the Criminal Division was here two weeks ago. He suggested the Department was not currently investigating the alleged abuses at Abu Ghraib. I will submit questions to you about that too. But let me ask you this: Are you now investigating the abuses at Abu Ghraib Prison?

Mr. MUELLER. We are not investigating those abuses. My understanding is that the military is investigating those abuses.

Senator LEAHY. You have not received any referral from the Department of Defense involving the nonmilitary contractors?

Mr. MUELLER. We have not received a referral.

Senator LEAHY. How many FBI agents are in Iraq?

Mr. MUELLER. I prefer to provide that information, if I could, Senator, off the record.

Senator LEAHY. All right. On May 13th the New York Times reported the interrogation methods employed by the CIA are so severe that senior officials of the Federal Bureau of Investigation have directed its agents to stay out of many of the interviews of the high-level detainees. The article also states that, "FBI officials have advised the Bureau's Director, Robert Mueller, that the interrogation techniques which would be prohibited in criminal cases could compromise their agents in future criminal cases."

Did the FBI direct its agents to stay out of the CIA interviews of high-level detainees because of the brutality of the interrogation methods being used?

Mr. MUELLER. Senator, it is the FBI's policy to prohibit interrogation by force, threats of force or coercion. Where we have conducted interviews, we have adhered to that policy.

Senator LEAHY. More specifically though, my question was: did the FBI direct its agents to stay out of CIA interviews specifically because of the brutality of the interrogation methods being used? Yes or no.

Mr. MUELLER. Our agents—

Senator LEAHY. That is what the press reported.

Mr. MUELLER. Our agents are under direction to adhere to the training and the directions that they have had in terms of how to handle interviews. In the case where we have been handling interviews, particularly over in Iraq, it has been done according to our standards and there has been no waiver of that.

Senator LEAHY. I will ask the question for the third time. Did the FBI direct its agents to stay out of the CIA interviews of high-level detainees because of the brutality of the interrogation methods being used? Yes or no?

Mr. MUELLER. The FBI has—

Senator LEAHY. It has been reported—

Mr. MUELLER. If I might, sir, the FBI has directed its agents to conform to its policies with regard to the handling of interviews, whether it be here in the United States or overseas, and to the extent that an agent believes that interviews were not being conducted according to the standards of the FBI, that agent was not to participate in those interviews.

Senator LEAHY. Let me ask you just for the fourth time, for the fourth time. Did the FBI direct its agents to stay out of the CIA interviews of high-level detainees because of the brutality of the interrogation methods being used?

Mr. MUELLER. No.

Senator LEAHY. Thank you.

Mr. MUELLER. But I will say that—again, I will go back—and the way the question is phrased, no, but I want to be absolutely clear that agents of the FBI were to participate where they believe that

the interrogations would be done according to the standards that we have set in the FBI.

Senator LEAHY. Were they told to anticipate that those standards would not be followed in CIA—

Mr. MUELLER. No. My understanding is that there are standards that have been established by others legally that may well be different from the FBI standards, and if that were the case and there were a departure from the FBI standards, we were not to participate.

Senator LEAHY. What others?

Mr. MUELLER. What others?

Senator LEAHY. You said that there are some interrogations that do not follow your standards. What others? By whom?

Mr. MUELLER. DOD and CIA.

Senator LEAHY. That is basically my question. So it is true the FBI agents are—

Mr. MUELLER. But my saying that, let me add, Senator, that that does not necessarily mean that those standards were not—that those standards were unlawful. What I am saying is that they may not conform to what we—the standard that we use in conducting investigations in the FBI.

Senator LEAHY. Your standards are set out, and agents are instructed not to take steps that would compromise them in a criminal case; is that a fair statement?

Mr. MUELLER. I think that is part of it, yes. But also, I mean, for a variety of reasons, our standards relating to interviews and interrogations are based on our belief on what is effective, our belief on what is appropriate, our belief on—and part of the footing of that is, quite obviously, the fact that we would have to testify in court on standards of voluntariness and the like. So our standards may well be different than the standards applied by another entity in the United States.

Senator LEAHY. And have any of your agents encountered objectionable practices involving the treatment of prisoners in Iraq, Afghanistan or Guantanamo?

Mr. MUELLER. We have conducted investigation to determine whether or not any of our agents in Iraq were aware or was aware of the practices that we have seen in the media, practices between I believe October 1st and December 31st of 2003, and we have interviewed each of the agents that conducted, may have conducted interviews in the Abu Ghraib Prison, and none of those witnessed abuses such as we have seen.

Senator LEAHY. Let me ask you this. Is the FBI conducting any investigations involving handling of prisoners in Guantanamo?

Mr. MUELLER. No.

Senator LEAHY. None?

Mr. MUELLER. We are not conducting any investigations into the handling—

Senator LEAHY. Have you conducted any?

Mr. MUELLER. No.

Senator LEAHY. And you are not doing any in Iraq?

Mr. MUELLER. We are not.

Senator LEAHY. How about Afghanistan?

Mr. MUELLER. No, not to my knowledge. We are not conducting investigations into the handling of prisoners in either of those three countries. My understanding is that there is a referral, there has been a referral to Justice by the CIA, which I think has been made public, of certain issues, but the investigation has been conducted by the CIA Inspector General.

Senator LEAHY. So if they refer a case to Justice, you do not get involved in an investigation? I mean does it sort of sit there in Justice or what?

Mr. MUELLER. No. I think if there are referrals and Justice believes that we are the appropriate investigating body, they would ask us to conduct an investigation.

Senator LEAHY. So even though they have had cases referred to them by the CIA, they have not set them on to you?

Mr. MUELLER. My understanding is the investigations had been conducted to date by the Inspector General's Office.

Senator LEAHY. The same New York Times article says the CIA's coercive interrogation techniques were authorized by a set of secret rules adopted by the administration after the 9/11 attacks for the interrogation of high-level al Qaeda prisoners. The article states that these rules were endorsed by both the Justice Department and the CIA. Were you or anyone else at the FBI consulted about these rules?

Mr. MUELLER. I do not believe so.

Senator LEAHY. Did you or anyone else at the FBI endorse these rules?

Mr. MUELLER. No.

Senator LEAHY. You have no FBI investigations of military contractors regarding the handling of prisoners in any of the three countries I have talked about?

Mr. MUELLER. Not at this time.

Senator LEAHY. Have you had?

Mr. MUELLER. No.

Senator LEAHY. Do you have FBI at Guantanamo?

Mr. MUELLER. Yes.

Senator LEAHY. Afghanistan?

Mr. MUELLER. Yes.

Senator LEAHY. And Iraq?

Mr. MUELLER. Yes.

Senator LEAHY. Can you submit the information on that for the record?

Mr. MUELLER. In terms of numbers?

Senator LEAHY. Yes.

Mr. MUELLER. Yes. I would like to—not in open record, but I will absolutely submit it to the Committee, but we prefer to keep it not as part of the open record.

Senator LEAHY. Would you want to do it for the classified record?

Mr. MUELLER. Yes.

Senator LEAHY. I understand. We talked about the Trilogy Program, and we said that it has been updated, consolidated and so on. But we have spent in the 3 years since 9/11, $581 million, which is over budget, and long delayed. The Attorney General told Congress the virtual case files are on schedule to be implemented by December of 2003. You said the same thing in July 2003 when

you testified before us. In December the FBI told my staff it was delayed until summer. On March 23 of this year you told the Appropriations Subcommittee the FBI is still negotiating. Today you indicated the elements would be completed later this year. What elements and what do you mean by elements?

Mr. MUELLER. Let me go back, Senator. The contracts were entered into in the summer of 2001. We have had to undertake the modernization, given contracts were issued and entered into in 2001 prior to September 11th. There is an assertion that we have spent far more funds than were earlier anticipated, and that is true. The reason we have spent far more funds is because we have changed and adopted the program we need to put our information technology where it needs to be. We have completed, as Senator Hatch pointed out, a substantial portion of the Trilogy Project. We have put in more than 28,000 new computers. We have put in the local area networks, the wide area networks, the backdrop, the backbone of our system.

One of the things we have done that was not contemplated when we entered into the Trilogy Project is, early on, migrating our databases from the old ATA base, which is the foundation of ACS to which you refer, migrating that data over to modernized databases so it can be searched by search engines. That had not been contemplated prior to September 11th, and we have accomplished that.

The upgrade of our operating systems, which was to be completed by October, was not completed by October. We had what I believe to be problems with the contractor in that regard, and we went back and we negotiated a difficult finalization of that contract, and that was concluded on April 20th. We are in negotiations with the last contractor on the last piece of this program, the Virtual Case File, and my hope and expectation is that that will be completed by the end of this year.

But I do not believe, to the extent that you did say that we are not much better off today than we were before, that that is accurate. I do not believe that is accurate. I think we are much better off now than we were before.

The last point I would make is that when we entered into the contracts for the Trilogy Project, it was on a 3-year timeframe. I had originally, after September 11th, asked to move it up so that we could move faster. We are at the end of that 3-year timeframe, so compared to what we anticipated, we are pretty much online. It was my effort, my hope, my expectation that I could move up that timeframe some. As it has turned out, I was unable to do so, but I do believe that when we are concluded this year, we will have the foundation for the cutting-edge technology for an organization our size.

Senator LEAHY. Thank you, Mr. Chairman. I appreciate your courtesy.

Chairman HATCH. Thank you, Senator Leahy.

We will turn to Senator Grassley.

Senator GRASSLEY. Director Mueller, I really appreciate your work that you and your field agents are doing in the fight against terrorism. I also would like to commend you for the changes that you are making at the Office of Professional Responsibility. My

staff has been briefed on that. I may have a few little things to follow up in writing, but I wanted to acknowledge those changes.

The first question deals with the progress that the FBI is making in general in terrorism financing, and specifically with the Saudi Arabian financial activity. I chaired a Finance hearing yesterday on this issue. My staff has been investigating the Riggs Bank situation, and the money trail I think is very alarming. It looks like there are groups and individuals that have pretty solid links to terrorism who got money from the Saudi Embassy accounts at Riggs. I am sure that the FBI agents on this case are working as hard as they can, but I worry about political pressure may be impeding. Three points I would like to address, and I would like to give all three before you answer.

First, have you or senior FBI officials received any pressure or guidance from other agencies, including CIA, State Department or the White House to go easy on the case, and if you ever did, would you report that to Congress?

Second, please tell us in a general sense, because I know when you are dealing with a specific case you cannot talk about that case, but what kind of activity or involvement in terrorism financing is the FBI seeing from Saudi nationals and Saudi officials?

Third, what kind of coordination and effort is there from the FBI to dismantle al Qaeda financing as a whole as opposed to specific cases, especially in conjunction with the Treasury Department?

Go ahead.

Mr. MUELLER. As to the first question on political pressure, at no point in time have we received pressure from any other entity in the Government not to pursue every lead where it takes us. We would reject any pressure. It would not happen. It would not deter us from seeking out any fact that we need to further our investigation.

We have seen over a period of time Saudis, Saudi NGOs, NGOs that are headed by Saudis, contributing to terrorism. I think that is fairly well known over a period of time. We early on established a Terrorism Financing Operations Section that has been, I believe, very successful in integrating with, formerly, Customs, as well as with the Treasury Department, and undertaking a wide range of investigations into terrorist financing, and I might also say this is one of the areas in which we work exceptionally closely with the Agency and others, and we have been successful.

Lastly, with regard to the Saudis, before I turn to al Qaeda, we have had very good cooperation from the Saudi Government over the last year. We have a fusion cell in Riyadh looking at terrorism financing, and that has augmented our capabilities to address this particular problem. Looking at the financing of al Qaeda overall, I do believe that our efforts to go into Afghanistan and remove Afghanistan as a sanctuary for al Qaeda has had tremendous benefits in terms of disrupting their capabilities to recruit, to train, but also disrupting their capabilities to organize the financing along the lines that they were able to organize it prior to September 11th. Al Qaeda is fragmented. That does not mean that there are not individuals in this world who are not still providing financing to al Qaeda, but it is more difficult for them. And the efforts of not just the FBI but the other agencies in the United States, as well as our

counterparts overseas, has had a substantial direct impact on the funding of al Qaeda.

Senator GRASSLEY. In regard to your last point, because I ask in conjunction with the Treasury Department, has the Treasury Department been involved in those investigations?

Mr. MUELLER. Yes.

Senator GRASSLEY. As a conclusion on this point, today Senator Hatch and I, and Senator Leahy, and Senator Max Baucus, are sending you a letter asking to see Inspection Division reports on the FBI's legal attache in Saudi Arabia, and I look forward to seeing those reports. You do not have to comment on that now, but we are sending you that letter.

I would also like to, on a second point, figure out why the FBI is going back in time and classifying some pretty basic information that is already in the public sector in regard to classification of information that we have received in Congress from a whistleblower, Sibel Edmonds. We have, for instance, a e-mail sent out by the Chairman Office last week saying that the FBI is classifying 2-year-old information the Committee got in two previous briefings. Ms. Edmonds worked for the FBI as a translator, and was fired after she reported problems as part of the Committee's legitimate oversight. We looked into that. So I am very alarmed.

The e-mail I have is right here. I am very alarmed with the after-the-fact classification. On the one hand I think it is ludicrous because I understand that almost all of this information is in the public domain and has been very widely available. On the other hand, this classification is very serious because it seems like the FBI would be attempting to put a gag order on Congress. Frankly, it looks like an attempt to impede legitimate oversight of a serious problem at the FBI, and that makes it harder for the FBI's problems to get fixed. The so-called mosaic theory of classification can probably be applied to just about any information.

I do not think this is really about national security. If it were, the FBI would have done this a very long time ago, and in fact, you would be trying to get information back that has already been given to us about Ms. Edmonds.

The result of this retroactive classification will be a roadblock in front of Congressional oversight and the victims of 9/11 because I think that lawyers want to interview Ms. Edmonds. I think a better solution is for the FBI to face up to its problems with translation. I understand that there are tens of thousands of hours of untranslated material from this year alone, and that is just for Terrorism and Intelligence Committee. So I have two questions.

First, who is the primary decision maker for classification? Would it be Justice Department lawyers or operational people at the FBI? The second part of this is, how is this classification supposed to have any credibility when it is 2 years after the fact and all the information, it seems to me, is in the public domain?

Mr. MUELLER. Senator, I understand your concern about this particular issue. My understanding is that the information was provided to Congress sometime ago openly, 2 years ago, almost 2 years ago, and that there are other areas of information that have come out, that put together with that information, may bear on the national security, which is why that decision was taken. My under-

standing is it is a joint decision between the Bureau and the Department of Justice. I can assure you it is not in any way an effort to impede legitimate oversight inasmuch as the information has been provided to Congress some time back.

I might also add in that context that as I have in each case of a whistleblower in the past, I have referred the matter over to the Inspector General, and the Inspector General is conducting an investigation into all of these allegations. It certainly is not an effort to in any way interfere with either Congress's or the Inspector General's investigation, and as I have in the past, if there are recommendations that come out of that investigation, I will look at them and for the most part, as I have in the past, I will adopt them.

Senator GRASSLEY. My last question deals with the Chinese spy case in Los Angeles. I am not asking you about criminal case though because I know you are restricted on that. Former Agent J.J. Smith recently pled guilty to what seems like a light charge. It does not look like he is going to get much jail time. There have been some comments in the media about how this looks like a double standard and that has concerned me because we have discussed that in previous open hearings of this Committee. But I would like to focus on something else separate from the criminal case, and I would ask two questions.

First, can you tell me if any internal FBI misconduct allegations have been filed against current or former senior officials in Los Angeles or in headquarters relating to the Leung, how Leung was handled in other intelligence matters? And second, are these allegations being investigated by either the FBI or the Justice Department? I am asking this because I have received information that the FBI really did not property judge who was responsible for the problems of the double agent and who was to blame.

Mr. MUELLER. Two things. Immediately after this came to my attention, I asked for a quick review of individuals who are still in the chain of command in Los Angeles to determine whether or not I should take some action immediately. And there were, I believe, at least one if not more actions taken as a result of that review.

At the same time though, I asked the Inspector General to conduct an investigation and the Inspector General has been conducting an investigation for probably a year now into the events of what happened out in Los Angeles, and I would await the conclusion of the Inspector General's report to determine what further steps should be taken.

Chairman HATCH. Senator, your time is up.

Senator Kohl.

Senator KOHL. Director Mueller, we understand that the State Department and the FBI are active in providing security at the Summer Olympics, intended to be in Athens. We have heard many athletes expressing concerns about their safety, and it seems that there may be good reasons for them to be concerned. As you know, Greece is close to many interests hostile to the United States and the area, and Greece's borders, particularly those on the Mediterranean Sea are porous. These fears are only exacerbated by the numerous bombing attacks that have occurred in Athens over the

past year, some of which took place while you were there in November.

Given the situation and your knowledge of what is being done there in terms of security, what can you say to the American athletes who are concerned about their safety?

Mr. MUELLER. We are working with the Greek authorities. It is the responsibility of the Greek authorities to protect the Olympics. They are confident they have put into place the mechanisms to do so. We have been and will continue to work with the Greek authorities. We continue to monitor the progress with regard to the security of the Olympics. At this point in time, as I say, we continue to monitor it and see what progress is being made to assure that these Olympics are free from attack. I think it is too early for any dispositive judgment as to the substantial gaps in that security. To the extent that we have identified them over the last several months, 6 months or so, the Greek authorities are moving to fill those gaps, but as I say, we are continuing to monitor the situation there.

Senator KOHL. Is your concern a high-level concern?

Mr. MUELLER. Yes.

Senator KOHL. Do you think that there is substantial risk there?

Mr. MUELLER. No. When I say it is a high-level concern, I think all of us want to make these Olympics the safest possible Olympics, and I know the Greek authorities want to make these the safest possible Olympics. They are looking forward to having the Olympics go off without a hitch and not only ourselves, but a number of other countries are working with not only our ambassador, but ambassadors of other countries in Greece, to ensure that these can be the safest possible Olympics.

And when I say "high-level concern," it is a concern because all of us want to make these a safe Olympics and are willing to do what is necessary to make that happen.

Senator KOHL. Is it safe to say that the level of security at these Olympics will be perhaps higher than have ever been seen in an Olympics before?

Mr. MUELLER. I think that is probably fair to say.

Senator KOHL. Director Mueller, the last time we saw each other, we discussed a Terrorist Screening Center. I would like to say again how important it is to have one central watch list for terrorists to effectively protect against terrorist attacks and keep our law enforcement alert to known terrorists. Such a list should be available to border security personnel, State and local law enforcement and others who are charged with protecting our Nation.

You said, in March, that you expected a terrorist watch list to be fully integrated by this summer. Can you give us an update on where that is.

Mr. MUELLER. It was fully integrated as of March 12th. There was one integrated list as of March 12th. The next step in the growth of the Terrorism Screening Center is to make that list accessible directly on-line from each of the agencies.

Right now, every one of the agencies participating in the Terrorist Screening Center has communication to their particular fields, and the names come in, and then it is run against the list. By the end of this year, what we want to be able to do with appro-

priate security, quite obviously, is to have the centralized list, which we do have, accessible directly from the field, so that the field does not have to come in to their counterpart in the Terrorism Screening Center, but can go electronically right to the list and get the information that way, and that is the next step of the evolution of the Terrorist Screening Center.

Senator KOHL. Can you assure us that the FBI does not use any of the abusive interrogation methods that we have been reading about in Iraq here in the United States?

Mr. MUELLER. Yes.

Senator KOHL. Does the FBI have procedural rules governing the interrogation of prisoners captured here in the United States?

Mr. MUELLER. Yes.

Senator KOHL. Since September 11th, we have been collecting more intelligence and terrorist-related investigations. Terrorist organizations operate in the shadows of our society and are difficult to detect even when our counterterrorism people have all of the information in front of them. Their job is virtually impossible when the information we do have is not translated in a timely manner. What are you doing at the FBI to develop a long-term solution whereby the FBI can attract adequate numbers of qualified translators without compromising security?

Mr. MUELLER. We have put into place Tiger Teams, as we call them, over the last year, year and a half, to bring on board, first, recruiting and then bring on board numbers of translators in the languages where we have been weak in the past. We are going to continue to do that and augment our capability by seeking to attract and then hire a number of the translators in these particularly Middle Eastern languages. We have more than tripled our numbers of analysts in some of the more important categories, such as Arabic. Where we had, on September 11th, 70 Arabic contract linguists and language specialists, we now are well over 200. Farsi, we had 24, and the last count I had was 55. Pashtu, we had one. We now have at least 10, if not more. Urdu, we had 6, and we are up to 21.

And so we have enhanced our capability and the numbers of linguists, but we are still not where we need to go. We have put into place a network whereby cuts of intercepted conversations, for instance, can be pushed around the country to a language specialist that has a particular skill and that, in and of itself, will substantially enhance our ability to have our conversations, our intercepts translated.

The one point I would make is we have had, as in all things, we have had to do a triage. We have had to prioritize, and so the priority, quite obviously, is terrorism. To the extent that we have FISA intercepts or a Title III intercept in any way relating to terrorism, that is the first priority, and those conversations, particularly if they relate to ongoing, perhaps, operations, are done within I would say 12 hours.

There are other investigations where, because we do not have as many linguists as we would like, that it is not within 12 hours, but we have investigations, for instance, going into financing of terrorist activity and a variety of terrorist groups, and it does not have the same immediacy to have that translated—maybe listened

to, but not translated—with the same immediacy that we have with regard to an ongoing terrorism investigation, and so we have had to prioritize, and I expect we will have to continue to prioritize in the future. But we, along with the community, are working in a number of different ways to augment our capabilities.

Senator KOHL. Director Mueller, the FBI has been heavily criticized since 9/11 for not connecting the dots and preventing those attacks. You have done much to reorganize the Bureau and to hope that those changes will better enable the Bureau to detect and disrupt plots. You almost completely remove the FBI from drug enforcement, and we are told that many smaller criminal investigations, such as bank robberies, are being left to State and local officials. So where do you see the FBI going from here? Do you plan to scale back on the Bureau's involvement in any other areas of criminal enforcement?

Mr. MUELLER. Let me, if I could, just point out one thing. We have not completely left the drug enforcement arena. We still have—and I can get you the figures—a number of agents who still are focused on enterprise drug investigations. We participate in OCDETF, Organized Crime Drug Enforcement Task Forces, around the country. We participate in HIDTA projects around the country. So we are still operating in the drug program and will continue to do so.

What we have done is tried to eliminate the overlap between ourselves and DEA in addressing cartel cases, and by cartel cases I mean Mexican or Colombian cartel cases where there had been overlap in the past, and we are doing fewer stand-alone drug cases, and by fewer I mean cases relating to methamphetamine, Ecstasy, that do not perhaps relate to enterprises, but I would expect that we would still stay in the drug program for a long time to come.

We have had to focus our resources in the bank robbery area and the small white-collar crime area, and we have done so. I have given latitude to Special Agents in Charge of the various divisions to identify particular priorities and to best maximize that Special-Agent-in-Charge's resources to address that priority. It may be in one city that bank robberies are a substantial problem. It may be a problem in Los Angeles and not Boston or Portland, Maine, or Oregon and not Miami. And certainly working with State and local on the priorities, we would work on a Bank Robbery Task Force for a period of time.

And so what we have tried to do is be far more flexible in addressing the concerns of the local communities than perhaps we have done in the past, not driven by statistics, but driven by the threats in particular communities.

As we go forward as a Bureau, I believe we should look for areas in which we are uniquely situated to address the threats of the future, and I look to 2010, threats of the future, international threats, terrorism, trafficking in persons, yes, trafficking in narcotics, transnational-international white-collar frauds. And with our 52 field offices, with our coverage in the United States, we are uniquely able to work with our counterparts to address that kind of more likely threats in the future, and so I expect us to continue to maintain a strong presence at the local level, but be that inter-

section between the local level and the international threats that we are going to increasingly face as we go down this path.

Chairman HATCH. Senator, your time is up.

Senator Specter.

Senator SPECTER. Thank you, Mr. Chairman.

Director Mueller, in the brief 10-minute time frame, I would like to ask you about two subjects—one, the Director of National Intelligence and, secondly, about the PATRIOT Act, starting with the issue of coordination of intelligence information. There are many of us, myself included, who still believe that there ought to be an overall Director of National Intelligence. I compliment you and others who have moved to have more coordination now than before, and I tried to get this as part of the legislation for the Secretary of Homeland Defense.

If there is a judgment made to go to a Director of National Intelligence, do you think it would be better lodged in the CIA with the Secretary of Homeland Defense and the FBI or should there be a new office created, designated Director of National Intelligence, or is there some other way that you would recommend that it be done, if we get to the point of deciding that that has to be done?

Mr. MUELLER. I wrestled with this, and it is not the first time I have been asked about it. I think you start with some of the areas where I think we have made substantial strides. The Terrorist Threat Integration Center accomplishes for analysis, as opposed to collection, the integration and the all-source access to information relating to terrorism.

Senator SPECTER. Director Mueller, I have only got 10 minutes. If you are going to tell me why we do not need one, that is not my question. My question is, if we decide we do need one, what is the option you would recommend?

Mr. MUELLER. I am not certain I would recommend any of those options. I think, as I testified before the 9/11 Commission, I think there are pluses and minuses in each of those options. I will tell you, if there is a decision to make—one of the reasons I do not have an opinion on a DNI is because I am not thoroughly familiar with all aspects of military intelligence versus CIA intelligence. I just have not been exposed to that.

Senator SPECTER. Well, would you do this for the Subcommittee or for the Committee, at least for me. Would you think about it and give us your opinion? Because of all of those who have to make a judgment, none of us has as much knowledge as we would like to have, and I would say you are a high-level expert, and your opinion would be very, very weighty.

Let me move on now to the PATRIOT Act and start by agreeing with you about the importance of tearing down the wall so that when information was obtained under the Foreign Intelligence Surveillance Act and could have been used for a criminal prosecution, the prohibition was not sound at all, and we did make that important change. And I know that has liberated you a great deal.

I believe that legislation in this field is necessary. I was concerned that the act was adopted without hearings in this Committee and rather hurriedly on the floor of the United States Senate one Thursday night which I expressed at that time. And in order to give the leverage to law enforcement to be able to use the

PATRIOT Act, there has to be confidence that civil liberties are being protected at the same time.

And because I only have 10 minutes, I want to give you a more lengthy preamble than I would like to do. I ordinarily like to ask one question at a time, but I cannot do that in 10 minutes.

The provisions with respect to an order for books, records, papers, documents, et cetera, has been referred to as an administrative subpoena, and I am told that that does not require probable cause, and there has been understandably concern expressed about going after library books, although there has been some report that no effort has been made to do that, but just the potential is problemsome. But if the library books related to how to make a bomb by an individual who had other indicia of the appearances or evidence or probable cause for being a terrorist, I could understand that.

Let me shift now to the delayed notice provisions, where the language is that if the Court has reason to believe, which is a different standard than probable cause, I would be interested in your views as to what the difference is. And on the delayed notice provision, there are five reasons for the delayed notice. Four of them appear to be specific and sound. The fifth is a catch-all "otherwise seriously jeopardizing an investigation or unduly delaying a trial." Where I come to the question part, it is whether you can get along without that catch-all provision, which causes some serious concern.

And coming back for just a moment to the order requiring the books, et cetera, the PATRIOT Act just says that there shall be a specification that the records concerned are sought to protect against international terrorism or clandestine intelligence activities. It does not have, within the PATRIOT Act itself, the language which is in the Foreign Intelligence Surveillance Act, where there is requirement of facts submitted by the applicant showing that there is probable cause to believe, and then it says, "for the standards."

And the questions I have for you are, where you have an administrative subpoena, if, in fact, that is what it is for books, et cetera, where there is a law enforcement official looking for that information, could that individual not specify why the information is sought, which really comes to the level of probable cause. When we have had probable cause imposed upon the States in *Mapp* v. *Ohio*, a very different change for law enforcement, the necessity arose to educate police officers as to specifying why they wanted to go after a certain record or document or search.

So the questions are, number one, if the FBI is looking for an order on books, records, is it too much to ask the agent to spell out why that is being sought, perhaps not to rise to the level of probable cause, but at least some reason to give it? And is there a different standard, under delayed notice, on reason to believe? And could you do without the catch-all on Item 5?

Mr. MUELLER. Let me go back. One comment you made is that the PATRIOT Act was rushed. I know this Committee had a hearing previously in which it was brought up that Patrick Fitzgerald, the U.S. attorney in New York, was quoted as saying people say the PATRIOT Act was rushed from his perspective, and he was the

one that was handling the al Qaeda cases in New York, and he said the PATRIOT Act was not rushed. It was 10 years too late. And I just wanted to get that on the record that there is a belief that what the PATRIOT Act has done in breaking down the walls has been tremendously helpful to us.

Senator SPECTER. Mr. Director, I believe with you that there is plenty of time to legislate, but there was plenty of time to have hearings before the PATRIOT Act went to the floor. We do not overdo the work week here in the United States Senate. So there is plenty of time to do it if we do it.

Mr. MUELLER. Going to the issue of the delayed notice first. I do believe that it is a lesser standard than probable cause because it is delayed if the Court finds reasonable cause, which is less than probable cause, I believe, and it is a lesser standard, but I think it is appropriate, when you are going before a judge and saying that, for this set of circumstances, we want to delay a notice for 30 days or 60 days or 90 days.

Senator SPECTER. Why should there be a lesser standard?

Mr. MUELLER. You have it before a judge, and probable cause in that circumstance, it is not a search. It is a delay of a notice. And I do not believe that you need to go to the higher level where you are asking a judge just to delay notice for a 30- or a 60- or a 90-day period, and I do believe—

Senator SPECTER. How about going after the books?

Mr. MUELLER. In terms of going after books, I believe a standard of relevance is appropriate, so that the Court can look at the rationale, but not necessarily probable cause. We do not require, as you know probably far better than I do, that in a criminal context, a grand jury subpoena for the same materials requires a much lesser standard than probable cause. It is relevance to an investigation. I think that same standard should be applied when we are addressing terrorism.

Senator SPECTER. But even that standard is not in the PATRIOT Act.

Mr. MUELLER. No, it is not. It is in the criminal code.

Chairman HATCH. Senator, your time is up.

Senator Feinstein?

Senator FEINSTEIN. Thank you very much, Mr. Chairman, and thank you for being here, Director Mueller. As I have said before, you have always been a straight-shooter and answered the questions directly, and I, for one, really appreciate that.

I do want to, along the line of Senator Specter's questions, bring to your attention that on March 23rd, I wrote a letter to Attorney General Ashcroft and Director Tenet, and in that letter I indicated that I was increasingly concerned about the confrontational tone of discussions about the PATRIOT Act and the 16 provisions among the 156 which are set to expire in 2005. And I said it was my hope that we can carefully consider and thoroughly evaluate these in a timely fashion. And I wrote to him asking for his assistance that he ensures a critical and comprehensive review of the implementation, value and importance of each of the 16 provisions. I received no response.

I wrote a second letter the next month on April 28th with a copy of my prior letter. I received no response to that. Now, I am a sup-

porter of the PATRIOT Act, but if I cannot get from the Department of Justice what I ask for with respect to a careful and comprehensive evaluation of each of those provisions, I will be hard pressed not to support the reauthorization, and I just want to let you know that.

And I will give you, before you leave today, copies of those letters. Perhaps you can use your influence and see that I get a response.

Let me put on my Intelligence Committee hat for a moment. In 2002, we passed, in the intelligence authorization bill, a section known as 321, and that essentially required the DCI, in its capacity as the head of the intelligence community, to develop standards and qualifications for those engaged in intelligence activities at the 15 departments.

And the report that we published went on to say, "The Committee," the Intelligence Committee, "has become concerned that, particularly in the area of analysis, elements of the intelligence community are denominating individuals as analysts or intelligence analysts without adherence to a meaningful and common definition of the word. Since September 11th, the Committee has been struck by the ever-growing number of individuals who are intelligence analysts, particularly in the area of terrorism. It is the Committee's intention to require the Director," that is the DCI, "to ensure that individuals performing analytic or other intelligence functions meet clear and rational minimum standards for performing those jobs."

My first question is has the DCI provided you with the communitywide standards and practices required by law?

Mr. MUELLER. I know we are putting—I am not certain of exactly the way the import of that law has been transmitted to each of the agencies that fall within the DCI.

Senator FEINSTEIN. I am talking about you, Director Mueller.

Mr. MUELLER. Yes.

Senator FEINSTEIN. It seems to me these standards should go Director-to–Director not through lower echelons. My question, and the intelligence authorization bill is very specific, have you been provided with communitywide standards for the hiring of intelligence analysts?

Mr. MUELLER. I do not believe so. We have established our own, in conjunction with the rest of the intelligence community.

Senator FEINSTEIN. So you would not know how many FBI analysts meet those standards.

Mr. MUELLER. We have been doing an assessment. I would have to get back to you on that.

Senator FEINSTEIN. I would appreciate that, if I may.

Mr. MUELLER. Yes.

Senator FEINSTEIN. I want to just follow up on a couple of things. What responsibility does an FBI agent serving in Iraq, Afghanistan or, for that matter, any other place have to report conduct such as we have seen at the prisons, and it is not the only one prison, but in other prisons, to report conduct that may violate United States laws?

Mr. MUELLER. It is to report it and to report it up the chain.

Senator FEINSTEIN. Have you received any reports?

Mr. MUELLER. From Abu Ghraib, no.

Senator FEINSTEIN. From any other prison or detention or interrogation facility?

Mr. MUELLER. We have, upon occasion, seen an area where we may disagree with the handling of a particular interview, and where we have, my understanding is—and we are still investigating—where we have seen that, we have brought it to the attention of the authorities who are responsible for that particular individual.

Senator FEINSTEIN. You mentioned in response to Senator Leahy that you had questions about the effectiveness of coercive interrogation. Can you explain that a little bit further?

Mr. MUELLER. I think there may be various bodies of opinion as to what is the most effective way to obtain information. There are certainly differing points of views. One of the points of views in the FBI is that developing a rapport may be as effective or more effective than other ways. That does not necessarily mean that our particular view, in a particular circumstance, is right. But as I expressed to Senator Leahy, in the course of FBI interviews, there are standards that FBI agents are to apply.

Senator FEINSTEIN. In April of this year—

Mr. MUELLER. May I add one other thing, also? And that is one of the things I do think it is important to understand is that our standards are developed with the understanding that, for the most part over the years, we have—and will continue—to conduct interviews within the United States—within the United States—under the Constitution, understanding that our mission is somewhat different than the mission of the Department of Defense and the CIA overseas. And so our standards we adhere to within the United States because that is our principal mission.

Now, in the case where we also are overseas, we ask our agents to adhere to exactly the same standards, and there have been no waivers of those standards.

Senator FEINSTEIN. Well, let me just say this: I admire you for taking the position that your agents are not going to participate where those standards are not present. So I thank you for that.

In April of this year, the FBI issued an intelligence report entitled "Threat Assessment, Los Angeles." I have reviewed the report carefully, and while the details are classified and I will not go into them, I wrote to you earlier this month to express my concern, saying in a letter dated May 3rd that, although titled "Threat Assessment," the report contains little intelligence analysis; rather, it is a combination of older intelligence data and random comments on ongoing investigations.

In essence—and this is a problem, I think, with your agency—rather than analyze the implications of the data you have, the report counts the number of open investigations. In my view, counting investigations is a valuable law enforcement tool, but it is not a substitute for analysis.

How is the FBI going to address this problem and acquire the skills that are necessary to do real intelligence analysis? Wouldn't an assessment of the threat to Los Angeles be primarily based on foreign intelligence collected overseas with the information from your investigations being added data?

Mr. MUELLER. I think that is a valid criticism, and too often in the past I think what we have done is look at the number of cases, and that does not substitute for the analysis that you describe. And I would think a thorough analysis would include not only information from overseas and not only the number of cases we have, but also input from our sources in that area, whatever sources contribute to that, and give an overall assessment.

I think you will be seeing one relatively shortly, and throughout the Bureau, we are gaining that capability not only by hiring analysts who have that capability, but through the College of Analytical Studies and from our intersection with both TTIC, as well as the CIA, as well as also the NSA.

We have put out a number of, I think, very good assessments. The assessment we did on the national threat domestically over the last year I think has been a top-quality product. And as we continue to grow our capabilities there, I think you will see the quality of the product will be much improved as we gain the capacity.

I will tell you that we have put in each of our offices a field intelligence group with reports officers, with persons in those intelligence groups who understand how to put together an assessment. That is not a capability that we have had in the past, and we are building it. We are not where we want to be, but we are building it and we are building it as fast as we can.

Chairman HATCH. Senator, your time is up.

Senator FEINSTEIN. Thank you. Thank you very much.

Chairman HATCH. Senator DeWine?

Senator DEWINE. Thank you, Mr. Chairman.

Mr. Director, thank you for joining us. I know that you have expanded the Trilogy information technology program as a result of the Webster report on Hanssen, September 11th, and other issues. As a result, the FBI was allowed to reprogram certain funds to address this expanded focus. Let me ask you a couple specific questions.

After redirecting these funds, do you currently have enough money to complete Trilogy? What will be the total cost of Trilogy? How much money do you have left to spend on the program? And when will Trilogy be completed?

Mr. MUELLER. I am not certain I have answers today on each one of those questions. I believe we do have sufficient money. Let me check one thing.

[Pause.]

Mr. MUELLER. I believe the total cost, as I pointed out before—but we have had some enhancements that we have included in that—will be close to $560 million, and the last piece of Trilogy, that is, the Virtual Case File, my expectation is that it will be in by the end of the year.

Senator DEWINE. End of this year?

Mr. MUELLER. This year.

Senator DEWINE. I understand that the FBI commissioned the National Academy of Science to evaluate the Trilogy plan. They were fairly critical. However, I also understand that many of these criticisms are for issues the FBI may have already addressed. The NAS does not dispute that possibility, but indicates they have been

unable to determine the FBI's progress because the FBI has not been forthcoming on these issues. That is what they say.

Can you address these concerns?

Mr. MUELLER. Well, I do think we have been forthcoming on the issues. One of the things about the report is that it was done 6 months ago, and there have been substantial changes in terms of the development of an enterprise architecture, the appointment of a new chief information officer, different mechanisms to assure higher-level input into the project, all of which were recommendations that were in the report as it was drafted 6 months ago.

The panel is coming back together to evaluate the progress that has been made since they last drafted the report, and my expectation is that there will be acknowledgment of that in the next several weeks, in a supplemental or an addendum to the report.

Senator DEWINE. So we should wait for that?

Mr. MUELLER. Yes, sir. On the other hand, we would be happy to brief, as we have others, where we are on our information technology, the good and the bad. And there have been some tremendous bright spots; there have been a number of—a relatively few bumps in the road, but there have been bumps in the road.

Senator DEWINE. You and I have discussed that before. I appreciate that.

Let me switch gears here a minute. Once September 11th happened, the FBI, as you have testified in front of this Committee on several occasions in the past, fundamentally shifted gears, and you moved from a reactive agency to a proactive agency, and you moved from an agency that dealt with many, many different things to an agency that has focused to a great extent today on terrorism.

Every time you are here, Mr. Director, I ask you this question, and I am going to keep asking you this question because I think it is important for the American people to understand the answer. And I suspect the answer will continue to change a little bit.

What is it that the FBI is not doing today that you were doing in the past? What is not getting done now because of this change in direction? You are doing more. You are doing more in the area of terrorism, fundamentally more. You do have some more resources that we have given you.

Mr. MUELLER. Yes.

Senator DEWINE. But that means some things still are not getting done or are not getting done as well. Candidly, tell us about that.

Mr. MUELLER. We are not doing—

Senator DEWINE. The American people need to know that.

Mr. MUELLER. Yes. We are not doing as many drug cases. I think that is—to the extent that there is some impact, I think it is probably more in middle America because of the predominance of methamphetamine as a drug of abuse. And we have better coverage in most of middle America than the Drug Enforcement Administration does, and so that has fallen to State and local law enforcement. So we are not doing as many drug cases. We are not doing as many cartel cases. But I do believe that the slack on the cartel cases has been picked up principally by DEA.

We are not doing as many bank robberies. We are not doing the smaller white-collar criminal cases, the bank embezzlements under

a couple hundred thousand. I hate to say it here, but we are not doing as many smaller white-collar crime cases as we were doing before. We are relying more—and when I say "we," I would say law enforcement is relying more on the Inspectors General to investigate fraud and abuse against the Government.

Those are some of the areas in which we are doing far less of than we had done in the past. But as we continue to stress that our principal priority is addressing terrorism, Congress and the administration have given us additional resources in terms of agents and analysts in counterterrorism that have then freed up agents who had been redirected from those other programs to go back to some of these criminal programs.

But in the future, my belief is our three principal priorities—counterterrorism, counterintelligence, and cyber—will continue to draw additional resources from some of the other traditional areas that we have handled.

Senator DEWINE. And the reality is that what the FBI always brought to the table was the ability to handle the complex case, the long-term investigations. And when you hand those off, by necessity now, to local law enforcement, that means somebody has got to pick up long-term investigations. And sometimes that is difficult, frankly, for local law enforcement to do, and that is just a fact.

Mr. MUELLER. It is, and—

Senator DEWINE. That is a fact. That is where we are.

Mr. MUELLER. It is. One of the things I stress to each of the Special Agents in Charge is that when you sit down with your local police chief, there may be a gang problem, there may be a particular drug problem, and there is no reason why we can't bring the capabilities we have to bear on that problem for a period of time until it is addressed. But we should not stay in task forces beyond the time that we can contribute. And we ought to be more flexible in addressing those particular needs of State and local law enforcement with some particularity as opposed to trying to do it with a broad brush.

Senator DEWINE. Let me move to one final question, and that has to do with the whole FISA process and changes that have taken place there. How are we doing there? Do we need to make any change in the FISA law, in your opinion? How are we doing? And do we need to make any changes?

Mr. MUELLER. Well, there is the Senator Kyl—I think it is the Kyl–Schumer statute that is still pending that I think would be of substantial benefit were we to have that passed. I would have to get back to you on that. I know that lone terrorist is one of the issues—

Chairman HATCH. That is the lone wolf—

Mr. MUELLER. That is the lone-wolf piece of legislation.

Senator DEWINE. Right, and we hope to give that to you.

Mr. MUELLER. And I have to get back to you, again, and look at that. It is not right on my mind at this point.

Senator DEWINE. Could you take that then as something that you will get back to us in writing on?

Mr. MUELLER. Absolutely.

Senator DEWINE. We would appreciate that.

Mr. MUELLER. If you can excuse me just a second.

[Pause.]

Mr. MUELLER. Specifically with the FISA statute, that is right. I have to get back to you on that.

Senator DEWINE. What is your analysis, Mr. Director, of how FISA is working mechanically now?

Mr. MUELLER. It is working—

Senator DEWINE. The flow, because I do not want to in an open hearing get into too many details. But—

Mr. MUELLER. Let me just say there are two components to it, and that—

Senator DEWINE. I have some concerns.

Mr. MUELLER. We still have concerns, and we are addressing it with the Department of Justice. And I can tell you one thing: the quality of work is as it has been in the past. We have had to prioritize in ways that we have not in the past. And we have had to add additional persons, and part of the challenge is both from information technology as well as the training and augmentation of the FISA staff, whether it would be in the FBI or in DOJ. We have recently embarked on a task force concept that I think will do much to ameliorate the problem. But there is still frustration out there in the field in certain areas where, because we have had to prioritize, we cannot get to certain requests for FISAs as fast as perhaps we would have in the past.

Senator DEWINE. My time is almost over. Let me just say that that is something that, Mr. Chairman, I think this Committee should spend a little more time looking at. When the Director of the FBI comes into this hearing—and we are in a open hearing and cannot go into any great detail. But it is clear there is a frustration level here with the Director, and it is clear there is a frustration level with people in the field. And when he is talking about making priorities, that tells me once again that things are not getting done out there. And we are going to be looking up, Mr. Chairman, in a year or two from now, and we are going to be looking back at things that did not get done because of some mechanical problems out there that should have been fixed. And something is wrong out there.

Chairman HATCH. I agree.

Senator DEWINE. There is just a problem here.

Chairman HATCH. Senator, I think that is a good point.

Senator Feingold?

STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator FEINGOLD. Thank you, Mr. Chairman.

Director Mueller, I appreciate working with you, I enjoy working with you, and I admire the challenges you have and the way you are meeting them. So it does pain me to hear you using the same approach that almost everyone else in the administration uses to defend USA PATRIOT Act. I have heard the President do it; I heard the Attorney General do it.

You say the bill has to be reenacted in exactly the same form. Then you cite a bunch of provisions, Mr. Mueller, that nobody objects to. It is a bait-and-switch. Nobody is against taking down the wall. Nobody wants to put the wall back up. Nobody does. I never

did. When I voted against the bill, I never suggested—in fact, that was one of the provisions I was enthusiastic about.

Then you cite the idea on the roving wiretaps. Everybody in this Congress wants us to be able to get at the other telephones. No one suggests that you should only be able to get at one telephone in an era of cell phones. It is simply not anything that anyone has proposed that I know of. Nobody opposed the idea of nationwide search warrants, the sort of thing you mention.

And here is the problem. The problem is that you suggest to the American people that somehow these provisions are in dispute, that you, I am sure, properly have indicated have been helpful. But the provisions that we are concerned about—and Senator Specter actually mentioned some of them—do have problems with the drafting.

Now, you may be right that some of these provisions took 10 years to get them to us, but I assure you that our part in the process, which I think is still important, was extremely rushed, and the language was not carefully reviewed.

For example, you take the sneak-and-peek searches. Senator Specter mentioned this. The PATRIOT Act could allow delayed notice of a search for potentially an indefinite period of time. In other words, instead of a judicial review and monitoring on a 7-day basis to make sure that it is still needed, it is indefinite. Now, that is not something that you have shown any evidence to suggest is necessary in order to protect us from terrorism.

It also has the catch-all provision that Senator Specter mentioned that allows delayed notice of a search if it would "seriously jeopardize an investigation or unduly delay a trial." Well, that is just too broad without a specific connection to terrorism.

So the point here that I want to make—and the same goes for Section 215. You started talking about a relevance standard regarding the library records. There is no relevance standard for Section 215. It simply says if you, the FBI, say you seek the information in connection with the investigation, the judge is required to give you the order. And I have heard the President and the Attorney General all suggest that somehow there is genuine judicial review there.

So the point here is that I don't think you even really want the USA PATRIOT Act passed exactly intact again. There is a necessary process that many members of this Committee are engaged in on both sides of the aisle—Senator Craig, Senator Specter, Senator Durbin, myself, and others—where we want to fix the USA PATRIOT Act. And the problem is the approach you are taking enhances the view of many people in this country that you are not trying to fix it, that you are just defending it at all costs. And I think that is a mistake. I think that is a mistake for the Constitution. I think that is a mistake for what you are trying to do.

Let's give the American people an opportunity to believe that you and this administration have a concern about some problems with the powers, and let's fix them so there can be confidence as we all go forward to fight terrorism.

In that spirit, I thought until today—and I certainly hope after your answer I feel again—that you believe there is a need for dialogue about these issues. I was pleased when you agreed to speak

apparently at an ACLU conference about the PATRIOT Act. Earlier this week, William Safire wrote a column about his concerns with data mining and made a point about balancing security with liberty that I believe also applies to the debate in the PATRIOT Act. He warned that, "In obtaining actionable anti-terror intelligence, there is a connection between, one, today's concern for protecting a prisoner's right to humane treatment and, two, tomorrow's concern about protecting a free people's right to keep the government from poking into the most intimate details of their lives. Must we wait until intrusive general searches mushroom into scandal, weakening our ability to collect information that saves lives?"

So, Mr. Director, do the American people have to wait until a scandal occurs? Or wouldn't you agree that the administration should be taking concrete steps now to address the legitimate concerns that have been raised on both sides of the aisle about the language of the PATRIOT Act? And are you willing to sit down with a group of us who are cosponsors of the SAFE Act to talk about it?

Mr. MUELLER. Well, Senator, you started off by saying that the roving part of the statute is not at issue, but part of the SAFE Act would modify that part.

Senator FEINGOLD. I didn't say that, Mr. Director. I said that the issue that you brought up of being able to get at multiple telephones is not at issue.

Mr. MUELLER. Okay.

Senator FEINGOLD. So this is what this is all about. You cannot just say that making one criticism of one part of the provision means that we think the whole thing should be thrown out. That is not our position. That is not what we are trying to do. We want to fix it, Mr. Director.

Mr. MUELLER. And I would acknowledge that a debate is appropriate. I would be happy to sit down with you or any Senator here to discuss what changes are appropriate. But what my concern is about is the heart of the PATRIOT Act. The heart of the PATRIOT Act. And I look at some of the modifications in the SAFE Act, and I would disagree with you and I disagree adamantly in terms of taking out the last provision, (e), where the judge—you call it sneak-and-peek, but delayed notification, where a judge can delay notification because, as it is in the PATRIOT Act, it would seriously jeopardize an investigation. And for most times in which this has been approved previously by judges, it has been under that standard because that is what most concerns us.

I am happy for the debate. I am glad to sit down with you or any of the other Senators to debate the provisions. But in my mind, what has not been acknowledged—and I wish it were acknowledged—is that the PATRIOT Act has made us safer as a whole.

Senator FEINGOLD. I want to say to you that I have never said that certain provisions of the PATRIOT Act don't make us safer, and that is not the debate. I only raised in my opposition to it a handful of provisions that I think are terribly important. But let's just agree that there are many provisions, all the way from being able to get voice mails because you could get the regular conversations of people, the border guards for Canada. That is not helpful

to the debate in our country to suggest that those things are not important.

What I think you just did is helpful. Let's get down to the actual language. Is there a way in which we could both agree on that language, maybe make it tighter and make it less of a catch-all that would still address the concerns you have? And I do appreciate the fact that you are willing to meet with us and talk about those.

Let me switch to the questions that the Ranking Member asked a bit about Iraq. Could you please tell us where the agents and translators and other employees were assigned before they were sent to Iraq? Were they working here on stateside issues relating to terrorism, or were they pulled off of active investigations or diverted from assisting in other matters?

Mr. MUELLER. They will have come from offices around the country.

Senator FEINGOLD. They were from here?

Mr. MUELLER. From the United States.

Senator FEINGOLD. Were they already working on terrorism-related issues?

Mr. MUELLER. Some of them were. Some of them may not have been.

Senator FEINGOLD. Well, the President said, correctly, that the fight against terrorism is not a war against Islam or the Arab world, and I appreciate your references to this today. I feel very strongly that the message should be sent repeatedly to the world as well as to Americans here at home. I am concerned that there are still some in this country who have misinterpreted this fight against terrorism and this conflict in Iraq as a war against Muslims or Arabs.

Last week, the American–Arab Anti–Discrimination Committee sent you a letter asking you to issue a public statement to quell the public fears about hate crimes against Arab and Muslim Americans in light of the recent events in Iraq. Mr. Director, as you know, protecting civil rights is one of the FBI's top priorities. What can you say today to the public to remind them that we are not engaged in a war against Islam or the Arab people? And what you say to reassure Arab and Muslim Americans that the FBI is, of course, committed to protecting their civil rights?

Mr. MUELLER. Well, as I said at the outset, the war on terror in the United States has to be undertaken by all of us, and for the most part, it requires us to be alert, vigilant to persons in our communities that might want to either support or undertake terrorist acts. And all of us together have to understand the responsibility, and the Muslim American and the Arab American communities have understood that and work closely with us.

Each one of our SACs, Special Agents in Charge, has gone out since September 11th and developed, I think, good, close working relationships with members of these communities, and we will continue to do so. It is tremendously important.

On the other side of the line is the assaults that have occurred on members of the Arab American and Muslim American community that are especially heinous in the light of what happened on September 11th, and since September 11th, we have initiated 532 hate crime investigations where the victims were either Arab, Mus-

lim, or Sikh. And out of those investigations, Federal charges have been brought against 18 subjects and local charges against 178 individuals.

So, on the one hand, we appreciate and we thank and hope to continue to work with the members of the Muslim American and Arab American communities who, as I have always said, are as patriotic if not more patriotic than most perhaps in this room.

And, on the other hand, to the extent that there are those who don't see that, don't understand it, and undertake hate crimes, we will be there, we will be investigating, and charges will be brought, and you will be doing time in jail.

Chairman HATCH. Senator, your time is up.

Senator FEINGOLD. Thank you, Mr. Chairman.

Chairman HATCH. But just to clarify before I turn to Senator Cornyn, 16 provisions of the PATRIOT Act are due to expire on December 31, 2005. Among the provisions that are subject to expiration are Sections 201 and 202, which add terrorist offenses and computer fraud or abuse as predicates to obtaining wiretaps; Section 203 and 218, which enable law enforcement to share counterintelligence information with the intelligence community; Section 206, which permits roving wiretaps; Section 209, which permits law enforcement officials to obtain voice mail through a search warrant rather than a wiretap; Section 220, which authorizes nationwide issuances of search warrants for wire or electronic communications and electronic storage and others.

If these provisions expire—and I am not saying the distinguished Senator from Wisconsin has been against all of these provisions—

Senator FEINGOLD. Mr. Chairman, that is simply untrue.

Chairman HATCH. I said I am not saying that you have said that you are against these provisions, all of these provisions.

Senator FEINGOLD. I just really—

Chairman HATCH. What did I say—

Senator FEINGOLD. Mr. Chairman, I want to be clear that I have not taken the position that all of these provisions should be—

Chairman HATCH. That is what I just got through saying, that you are not against all of these provisions, and that is what I thought I made clear. But you have been against some of them. And the critics have been against—I am just pointing out 16 very important provisions are going to expire, and that is all I wanted to point out. I find no fault with you wanting to have a dialogue and criticize. In fact, I do think we are going to have to have a hearing on the SAFE Act so that you can get that out in the open, which you would like to do, and, of course, have our law enforcement people tell us whether it is doable the way the SAFE Act wants it done or not doable the way the SAFE Act wants it done.

But one other thing. Anybody who thinks that the PATRIOT Act was done in haste didn't sit through the 18-hour days for 2 weeks, and years before, because it was the Hatch–Dole Antiterrorism and Effective Death Penalty Act where we debated some of those provisions before and could not get them in. I mean, this has been going on for years on this Committee, not just the approximately 18 days that it took day and night—you know, 18-hour days to do the PATRIOT Act. Those provisions we have debated for years, ever since I have been on this Committee. So it is not something that was not

well thought out or was not thought through. And the one thing that I think has to be said is that in the five hearings that we have held on this Committee so far, there has not been one—not one—effective criticism. The Senator from California made that point.

And, you know, we hear a lot of screaming in the media and a lot of criticism, but not one that has shown one misuse of the PATRIOT Act or one abuse of the PATRIOT Act. And I think that needs to be said.

Did you want to say something?

Senator LEAHY. Mr. Chairman, I would simply make this note taken from a somewhat different view. I was there when the PATRIOT Act—

Chairman HATCH. So was I.

Senator LEAHY. —was written, and I recall the first draft that came up from the Attorney General. You and others suggested we pass it that day. Some of us suggested we read it.

Chairman HATCH. I don't think I suggested that we pass it that day. That is not true.

Senator LEAHY. We will let the record—

Chairman HATCH. We worked the full time with your staff, and you know it.

Senator LEAHY. But be that as it may, after we read it, a number of changes were made to it by both Republicans and Democrats.

The point is that one of the major things put in it was the provision that has been referred to here, the sunset provision for December 31, 2005. This provision was authored by then-Republican Majority Leader Dick Armey of the House and myself. Now, we are not normally seen as ideological soul mates, but we authored it because these provisions were extensive and new, and we assumed that there would be real oversight on them. Part of the frustration with the Department of Justice is that a number of Senators on this Committee, both Republicans and Democrats, have written a number of letters about how some of those provisions were used—written to the Attorney General—and yet it does not respond or responds inadequately. I have stated before I think there is some huge room down at the Department of Justice where all these letters go.

But the reason they are there is to have real oversight. It is not a question of finding criticism. If you can't even answer the questions that were asked, nobody knows whether there is anything there to criticize or not, whether it is on FISA or anything else. Congressman Armey and I have written a letter jointly on the same question. He and I may or may not agree on every part of it. Senator Craig and I have written on this. We may not agree on every part of it whether it should go forward or not. We do not want to see ourselves in a Ruby Ridge-type situation. We do not want to see ourselves in any kind of a situation where we do not know the answers.

That is why the provisions are in there. That is why they will not be renewed, unless and until there is real oversight, which means, among other things, having the AG actually answer the questions.

Chairman HATCH. Before I turn to Senator Cornyn, let me just make the record clear, because in the FBI's report to the 9/11 Com-

mission, it indicates that a number of outside entities and individuals have studied the FBI's operations since September 11, 2001, and they have found no indication that the FBI has conducted operations with less than full regard for civil liberties. None.

For example, the DOJ Inspector General has issued three consecutive reports indicating that his office had received no complaints for each 6-month period alleging a misconduct by DOJ employees related to the use of any substantive provision of the USA PATRIOT Act.

Now, all I am saying is we are having an effective debate on this Committee. We are holding hearings. We are giving people from the left to the right an opportunity to criticize. To date, I have not heard one substantive criticism other than some would like to change one or more aspects of the PATRIOT Act.

I would suggest to everybody, listen to the Director of the FBI who has to live with those provisions and who has to protect us, along with his organization of 28,000 people. And I think if you do, we will have very few changes in the PATRIOT Act. But that does not mean we cannot make it better. If we can, I am going to do everything I can to do it.

Senator Cornyn?

STATEMENT OF HON. JOHN CORNYN, A U.S. SENATOR FROM THE STATE OF TEXAS

Senator CORNYN. Thank you, Mr. Chairman.

Director Mueller, thank you, and I admire you and the great work you are doing at the FBI. Of course, the debate we are having here now is one that we have had since the beginning of this country, the proper balance between security and liberty. And I think it is good that we have the debate. This is the right place to have it. But you shouldn't not have a debate in the FBI about executing the laws that are passed by Congress, and I appreciate the diligence with which the FBI is executing those laws and making us safer.

But I do take a different view than Senator Feingold expressed. I admire his sincerity and his conviction and his consistency, but I simply disagree. I think I for one will support an effort to strike the sunset provision in the PATRIOT Act because I think it ought to be made permanent, because I agree with you that it has made America safer.

But what I worry about is not people in Congress or elsewhere making good decisions about that balance between security and liberty based on good information or the facts. I worry about the facts being misrepresented or people being scared into making emotional decisions about what the PATRIOT Act does or does not do. And what I am referring to specifically is a campaign that has resulted in, I believe it is 287 different cities, city councils, municipal governments who have passed resolutions opposing—maybe "condemning" is too strong a word, but opposing the PATRIOT Act, including three in my State.

Then I happened to receive a solicitation for funds from the American Civil Liberties Union. I am not sure exactly how they got my address, but I did, and the primary thrust of that solicitation was that I needed to send the ACLU money to protect the country,

protect myself against the Government's use of the PATRIOT Act to somehow strip me of my civil liberties.

Of course, scare tactics are common. It is a way to motivate people to act. But it is not honest; it is not appropriate. And I think that the PATRIOT Act has made America safer.

I am amazed that we are having this debate, but, again, the debate is good. But after the 9/11 Commission hearings where you and the Attorney General and others talked about the importance of the PATRIOT Act's elimination or at least bringing down the wall that separated the law enforcement and intelligence-gathering agencies from information sharing and how important that has been. And it is amazing how you can see the public rhetoric and the public opinion kind of turn on a dime. It was as a result of that hearing which I think educated the American people about the good things the PATRIOT Act has done to make us safer. Indeed, I guess the best evidence of that is we have not, thank God, had another terrorist attack on our own soil since 9/11.

But let me ask you specifically about two things. One has to do with the material support provision of the PATRIOT Act. As you know, the Ninth Circuit has upheld a facial challenge to that provision of the PATRIOT Act, and other courts, of course, have rejected such constitutional challenges. And, of course, this material support provision of the PATRIOT Act actually precedes the PATRIOT Act. It had been applied and criticized since the Clinton administration.

But could you tell us the importance of retaining that provision or something very close to it in terms of the FBI's efforts to combat terrorism?

Mr. MUELLER. The material support statute is—I wouldn't say instrumental, but exceptionally necessary in order to prevent terrorist attacks. And the reason is because you cannot always hope to catch the terrorist with the dynamite in their hands going to the place where they want to undertake the attack. And you cannot wait until the person has the device together and wants to use it. You have to address terrorism by looking at the financing. You have to address terrorism by looking at the recruiting. You have to address terrorism by looking at the organization. You have to address terrorism by looking at the travel. And if you find persons who are supporting in one way acts of terrorism, then you need a mechanism to address that and to arrest them and charge them, give them their full rights under the Constitution, but address it.

One of the great problems in addressing terrorism is, you would say, it is somewhat of an inchoate crime. It is some place between somebody thinking up a terrorist act and actually accomplishing it. And it is between the thinking up of a terrorist act and having somebody accomplish it where we have to gather the intelligence to identify that person or persons and we have to make certain that they do not accomplish that terrorist act.

The other point about material support is that if one person commits a crime—it is like the conspiracy statute. One person commits a crime. The crime does not have the full force and effect as if you have a number of persons conspiring together to commit that crime. In order to be effective in 9/11, the persons who undertook that had to be financed; they had to have travel documents; they

had to have persons helping them in order to commit that final act on September 11th. And the material support statutes enable us to address that type of participant substantially before that terrorist act is on its way to complete. So it is very important.

Senator CORNYN. Not just the person that detonates the bomb, but the people who made that possible.

Mr. MUELLER. Who financed it, may have provided false identities, any number of ways that one can support a terrorist act.

Senator CORNYN. I have just one other question or area that I am just curious about. I know Senator Specter and others have talked—there have been proposals for a Director of National Intelligence. But I must say that in our effort to promote information sharing, particularly not just at the Federal level but at the State and local levels—and I do appreciate your emphasis on that in your opening statement because I do think that is critical. I worry that our intelligence community is sort of like the layers of an onion, it seems like. And I really don't understand—and maybe there are people smarter than I am who can explain it to me—why we would just want to add another layer to that onion when it comes to the intelligence community, how that would actually promote information sharing in a way that would make us safer.

Would you just comment on your views on that generally?

Mr. MUELLER. Well, again, I am Director of the FBI, not Director of CIA, but there is a belief—and George Tenet would articulate it—that in order to be effective, you have to be close to those who are doing the analysis, those who are doing the collection of the intelligence. And to the extent that you have someone that is divorced from that, you lose that effectiveness.

We have put into place mechanisms to enhance our analytical capability across all of our organization when it comes to terrorism. We have another mechanism—well, we have two mechanisms. One is the National Security Council and the Homeland Security Council. So to the extent that one needs operational coordination in any area, either the National Security Council or the Homeland Security Council does that coordination.

What I am less familiar with, do not understand fully, is the budget process in the intelligence community and how better coordination of that budget process might enhance the coordination of our intelligence across the Government. And there I just do not feel that I have sufficient information to provide much input.

Senator CORNYN. Let me just in quick follow-up, we, of course, have become familiar with the concept of jointness when it comes to fighting wars, joint training, joint operations. We have seen it in Afghanistan and Iraq between the various military branches.

Is it too simplistic to think that perhaps in intelligence gathering and analysis and dissemination we could conceive of the intelligence community's job is to act jointly? Is that the goal?

Mr. MUELLER. We have got to, regardless of whether there is a DNI. It will only be effective if we are working in a coordinated way between the Federal agencies, whether it be FBI, Department of Homeland Security, CIA, NSA, DOD, DIA. In order to be effective, we have to have an intersection of intelligence with State and local law enforcement. In order to be effective, we have to work with our counterparts overseas, whether they be law enforcement

or intelligence counterparts. And there has to be a sharing of information amongst all of these various players in ways that we have not in the past.

Senator CORNYN. Thank you, Director Mueller.

Thank you, Mr. Chairman.

Chairman HATCH. Senator Schumer?

STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Thank you, Mr. Chairman.

First, Mr. Chairman, let me thank you for holding this hearing in the morning, as I had requested. I appreciate that very much, and I want to thank the Director not only for being here but for the time he spent with me last week going over the progress FBI has made on computers. And I will have more to say about that at another time.

Today I want to talk a little bit about something that bothers me a great deal, and it will lead to a question to you, Mr. Director. Today, for the second time in as many weeks, there is evidence that a civilian contractor serving a senior position in the Iraqi prison system has a troubling history and a checkered record when it comes to prisoner abuse.

Last week, we learned that Lane McCotter, who was ousted from the Utah corrections system when a schizophrenic inmate died after being strapped naked to a chair for 16 hours, that is a practice that McCotter defended and affirmatively endorsed. McCotter then went on to serve as an executive in a private prison company that was under investigation for denying prisoners access to medical treatment and violating other civil rights. And at that point, after that checkered past, to be kind, Attorney General Ashcroft appointed him to help rebuild Iraq's prison system.

McCotter ended up being posted at Abu Ghraib where among his duties was the training of guards. This is a picture of McCotter along with Wolfowitz and Gary DeLand, and in the back is General Karpinski at Abu Ghraib.

So his appointment raised serious questions, including whether he had anything to do with the Abu Ghraib crimes. And I ask Attorney General Ashcroft what was being done to investigate the role of civilian contractors in the Iraqi prison scandal. I am still awaiting a response.

Now, today we learned—or I just learned this week that there is another leader of the prisons in Iraq with a similarly troubling past. So it makes the questions we have asked the Attorney General even more urgent. While running Connecticut's prison system, John Armstrong, here pictured in Iraq, made a practice of shipping even low-level offenders to a supermax facility in Virginia. It was notorious, this facility, for its use of excessive force. It ranges from the unjustified use of stun guns shooting 50,000 volts through prisoners—these are low-level—to locking inmates in five-point restraints for such lengthy periods that they were routinely forced to defecate on themselves.

Even after advocates objected and asked Armstrong to reconsider, he persisted in sending Connecticut prisoners to this jail where they were subject to treatment many have described as tor-

ture. Armstrong resigned as a result of the chorus of criticism over this decision.

But that was not all. When Armstrong resigned, he was under a cloud of credible allegations that he tolerated and personally engaged in sexual harassment of female employees under his command. One of the women who sued and claimed Armstrong had harassed her personally received a settlement of a quarter of a million dollars. And despite this record, Armstrong was tapped to serve as the deputy director of operations for the prison system in Iraq.

One official with a history of prisoner abuses raises an eyebrow, but two means we are really beginning to have a problem. Why would we send officials with such disturbing records to handle such a sensitive mission? That is beyond me. It cries out for explanation. Obviously, we have an obligation to ensure that all of those responsible are brought to justice, and we have a duty to guarantee that a handful of privates do not take the fall if they were directed by others. They should be disciplined appropriately, but when you read, for instance, what Sivits did today, that is, he was required or asked to escort prisoners to a certain place, he did not participate in what was going on—he saw it and did not report it to higher-ups—obviously, that is not sufficient.

This is unfair, and what bugs me the most, as somebody who really cares about our troops—I have traveled from one end of the State to the other and watched our troops go off to Iraq. I see them saying goodbye to their families, and they do it with a sense of duty, honor. And now wherever an American soldier walks overseas, these pictures come to other people's mind. It is unfair to them.

So we have got to get to the bottom of this, and if we are sending abusers, habitual abuses of what is normally conceded as rights, and putting them in charge of the prisons where we learned the abuses are now occurring, we need to know why it is happening and what is being done about it. We need to know if these men or others committed crimes in Iraq and whether they will be brought to justice.

As you know, if the FBI does not investigate and DOJ does not prosecute the civilians who committed these crimes, no one will. From what I understand, DOD may be saying it will investigate the crimes by civilian contractors and pass them along to the Department of Justice. That seems to me to be an unacceptable solution, Mr. Director. The DOD investigators know how to go after military crimes. That is their expertise. Civilian crimes, to be prosecuted in civilian courts, are a whole different story. We need professional prosecutors and criminal investigators on the job. We need them now. I would like to see us find out who did this, punish them appropriately, and move on. I say that as somebody who has been a supporter of the President's policies in Iraq, or at least supported the war and the money to go to the troops.

So the first question I have for you: Does it make any sense to have the DOD investigate civilians who cannot be prosecuted in military courts? Why shouldn't the FBI be doing this type of investigation?

Mr. MUELLER. Well, with all due respect, Senator, that was a lengthy statement before the question, and I do think it is a little bit unfair because you know that I cannot respond to the assertions you make, either about these individuals—

Senator SCHUMER. I am not asking that.

Mr. MUELLER. I know, but I do think it is unfair knowing that I cannot respond and defend either the individuals—

Senator SCHUMER. I am not asking you to do that. I am asking—

Mr. MUELLER. —or the Attorney General. And I would be happy to answer the question, but I do want to say that you and I know that I was not at all aware of this, what you are portraying today, that—

Senator SCHUMER. Well, the first one has been public for a week, McCotter.

Mr. MUELLER. In any event, I know that the Department of Justice is having discussions with DOD as to the jurisdiction. I do not know what the result of those discussions will be.

Senator SCHUMER. Here is what I want to bring out, and if I had gotten answers from the Attorney General, I would not be asking you these questions. But I am not asking you to comment on any individual case, obviously. The first one has been public for a week. It has been in lots of different newspapers and stuff. The second one we just came across today.

But if there are civilian contractors who may have broken the law, whoever they may be, does it make any sense to have DOD do the investigation? That is what I cannot figure out. They don't have jurisdiction.

Mr. MUELLER. Well, my understanding is they may have jurisdiction. That is being worked out. I do not know the basis on which they would have jurisdiction, and as in any investigation, it would be dependent on who you have to investigate. The general who investigated the abuses at Abu Ghraib did a superior job, and I think most persons in the Senate have said so.

Senator SCHUMER. Right.

Mr. MUELLER. And so, again, it is where the jurisdiction lies and who is doing the investigation, and I do believe that, as happened in the investigation of Abu Ghraib, a general or a person in the DOD can undertake a full, comprehensive investigation. But it really depends on where the jurisdiction lies, and that is being discussed.

Senator SCHUMER. Let's just take a hypothetical. A civilian appointee is involved in the prisons, gave the order to do things that violate the law to Iraqi prisoners. Why wouldn't we have the FBI do the investigation? Is there any doubt that DOD cannot discipline people who are not under military command?

Mr. MUELLER. Again, I would have to refer you to the Department on the jurisdictional issues, which they are working on now. My understanding is that there may be a basis upon which these individuals could be tried by the military, but I am not familiar with the arguments. And, again, I think it is still up in the air.

Senator SCHUMER. So you—okay. I will ask, Mr. Chairman, that I get an answer in writing from the Director if I am not going to get one from the Attorney General about whether DOD has jurisdiction. And if not—

Mr. MUELLER. I think there will be—I do believe there will be an answer. I am not certain that the answer has been fully clarified as yet. And I am not certain of the rationale or the reasons why we do not have—why there is no answer currently.

I can tell you, if requested, I believe we would be available to quite obviously investigate, but, again, it gets down to jurisdiction.

Senator SCHUMER. And all things being equal, if the DOD did not have jurisdiction to actually prosecute these folks, then wouldn't it make sense for the FBI to do the investigation rather than DOD and then turn over the information to—

Mr. MUELLER. Yes.

Senator SCHUMER. Thank you.

Chairman HATCH. Your time is up.

Senator Sessions, will be—unless Senator Durbin comes back—our last one.

STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. Thank you, Mr. Chairman.

On the question of the issue that Senator Schumer raised, Senator Schumer, I think all on this Committee supported the legislation that I offered in 2000 that became law to make contractors of DOD subject to criminal prosecution by the Department of Justice. I think the Act probably contemplated investigations being done by DOD in the field, but it also, I think, would probably allow FBI to investigate in the field. The ultimate prosecution would be by the Department of Justice. And I certainly have no concern or doubt that DOD can investigate it. I am familiar with the military legal system, the JAG officers and their abilities, and they are first-rate. I don't see any conflict of interest. The military is very upset about what happened in Abu Ghraib prison, and they want something done about it. So I think we will see that everybody that is guilty prosecuted.

I am glad that we had that statute passed. Without it, we would not have been able to prosecute. I do not believe these contractors could be prosecuted except perhaps in Iraq without this statute that we just passed a few years ago.

I think the contractors are not appointed by the Attorney General; however, I think they are appointed by the Department of Defense and those agencies. So I really do not think that Attorney General Ashcroft needs to take the blame for that. But I may be wrong.

Senator SCHUMER. Just if I could, McCotter was appointed by DOJ.

Senator SESSIONS. By DOD?

Senator SCHUMER. DOJ.

Senator SESSIONS. I have been asked a number of times, well, what about contractors? And I think the right approach is this: We need contractors. We need people who may be retired FBI agents who are willing to go to Iraq and help do the interviews and investigations. We need people who know how to run prisons that can help us in wartime run a prison. A young 19-year-old MP does not know the ins and outs of bringing up a prison and bringing it to operation. But we do need to monitor. And I think backgrounds are

important. Senator Schumer, I think you raise an important there. And, in addition to that, they need to be monitored in the field, and somebody needs to be in charge of them. That is one of the conclusions I reached about this prison system. We have yet to see—I think we will see who they are responsible to and who actually had control over them. But they have got to be disciplined just like any other official.

With regard to the PATRIOT Act, we have had a chorus of people going around saying all our liberties are threatened by the PATRIOT Act, as Senator Cornyn noted. So, first of all, we need to defend the Act. It is critical and valuable to us. The core parts of it are just absolutely essential. And I was pleased to see that Senator Feingold, who is a fine civil libertarian, agrees with the roving wiretaps and some of the other key provisions in there.

With regard to those issues that are somewhat in dispute, that are complained of, I think they are very small. But the sneak-and-peek is not a small issue. Do you agree?

Mr. MUELLER. Absolutely. It is a very important issue.

Senator SESSIONS. Now, you—

Mr. MUELLER. And they call it sneak-and-peek, and that is the wrong—it is delayed notification. Delayed notification. Delayed notification. They get these names, if you will pardon me just for a second, that are pejorative, that undercut the understanding of the public and exactly what is happening. And it is not that anybody goes in and sneaks and peeks. In fact, you get a court order to do a search. You do the search. And what you want it to do is delay the notification as you continue the investigation.

Senator SESSIONS. Exactly correct. So you have to have a search warrant submitted to a Federal judge with probable cause evidence that there is evidence of a crime inside the house or residence you want to search, and you can get those, and we have been doing those in America for hundreds of years, I suppose. Is that right?

Mr. MUELLER. That is correct.

Senator SESSIONS. They are done every day all over America. We see on television people raid a drug house or these law-and-order shows, they are always getting search warrants and judges approve them, and they go in and do their search.

Now, the difference here is simply that when you are dealing with a terrorist organization, the issue may be a life-and-death question. Is that right?

Mr. MUELLER. Correct.

Senator SESSIONS. And you want to maybe find out if there are pieces of a bomb being assembled in that house. And it may be important to protecting thousands of American citizens that we do not tell the bad guys, the terrorists, that very moment that we know and we are on to them; and that you would have the legal power to do the search, and you simply would not announce to the people searched that day that the search occurred. Isn't that what it is all about?

Mr. MUELLER. That is it. Simply, that is what it is.

Senator SESSIONS. I just think that is a critically valuable tool in terrorism investigations, and one of the things that happens is, as a former prosector myself, if you do the search too quickly, you tell everybody in the organization you are on to them. They know

you are on to the bad guys. And you do not want to do that sometimes. Sometimes that is critical that you not, and these kinds of delayed notifications were in place in the law even before the PATRIOT Act, were they not?

Mr. MUELLER. They were, and they were used in a number of different investigations, for instance, narcotics investigations where you do an investigation, an informant says there is in a locker some place an amount of cocaine. You do not want that cocaine to hit the street, but you have not completed the investigation. You get a search warrant, you go in, and you replace it with a white substance so it does not hit the street and you continue the investigation. And it has happened any number of time.

Senator SESSIONS. But even then, you have to ask a judge to allow you not to notify immediately. Isn't that right?

Mr. MUELLER. Yes, sir.

Senator SESSIONS. A judge would have to approve your decision not to notify.

Mr. MUELLER. Yes.

Senator SESSIONS. I do not understand the library. I mean, you can subpoena my bank records, my medical records, my telephone records. It is done every day in America by the thousands, every day. To say you cannot subpoena whether you checked out a book on bomb making from the library to me is breathtaking in its lack of understanding of the way the criminal justice system works. I do not see that librarians deserve a special protection here like priest and penitent.

Senator SESSIONS. Is there anything in the library of standards that you are aware of that represents an expansion or some sort of threat to liberty?

Mr. MUELLER. No. As I think you are aware, being a former prosecutor, in criminal investigations, a grand jury subpoena is allowable certainly to any number of institutions, including libraries, and the standard is basically a relevance standard. And so it is not new.

The one example is Kaczynski, who was the Unabomber, wrote manifestos. In those manifestos he had excerpts from books that were difficult to get. We were able, with the help of the library, to identify he was the person who had utilized those books and put together the fact that he had taken pieces from these books to put in his manifestos as he drafted, edited and submitted those manifestos while he was committing a series of bomb attacks throughout the United States.

Chairman HATCH. If the Senator will yield, it is new, with regard to the PATRIOT Act, in bringing the laws against domestic terrorism up to speed with other laws.

Mr. MUELLER. Right.

Senator SESSIONS. You are right, Mr. Chairman. That is the fundamental point of it.

Mr. MUELLER. Thank you very much.

Senator SESSIONS. Director Mueller, you are a professional. We are so glad you are here at this time in history. I have followed your career when we were United States attorneys, and I have seen you in the Department of Justice. I think there are few people in America that have tried as many cases, who has been involved

in as many investigations, long before you reached the august position you are in today, as a grassroots prosecutor, working with FBI agents, DEA agents, intelligence agents, and you are a professional. You were always known to be a professional. You were appointed United States attorney under the Clinton administration and under the Bush or Reagan administrations. You have a bipartisan reputation, and we are glad you are there.

Now, one thing I am concerned about, as we go forward with the entry-exit visas into America, the biometrics that are being discussed to bring some ability to make this system work. It seems to me that the United States, and most other nations of the world—

Chairman HATCH. Senator, your time is up, but if you would like to finish that one sentence, that would be fine, and then we will go to—

Senator SESSIONS. It seems to me that we need a system that stays consistent with our investment, which is fingerprinting. That has proven to work. We have got a system designed based on that. Should we not, as we expand our ability, make sure that the fingerprint utilization and computer system works for us with regard to entries and exits from America?

Mr. MUELLER. Yes, it has got to be. There has got to be interoperability and expansion of the system ourselves, working together with the Department of Homeland Security, to be on the cutting edge of the use of fingerprints and all of its various manifestations.

Senator SESSIONS. Thank you. It is utilized in every police department in America today, and it works extraordinarily well.

Chairman HATCH. Senator Durbin?

STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Senator DURBIN. Thank you very much, Mr. Chairman. Director Mueller, thanks for being here, and thanks for being so accessible and so candid in your answers, both before the Committee and in person.

Mr. Chairman, I might also note that this is a sad anniversary. It is almost 14 months now since the Attorney General has appeared before this Committee. I know he is a busy man and has extraordinary responsibilities, but so do Secretary Rumsfeld and Secretary Powell, and they have made themselves available before the appropriate authorizing committees time and time and time again.

I am troubled that, at this moment of national security being a major issue and concerns about constitutional liberties, that this Committee cannot possibly perform its constitutional responsibility if the Attorney General continues to refuse to come before us. I would hope that you would appeal to him, personally.

Chairman HATCH. Senator, he is going to come in June.

Senator DURBIN. Come in June, so it will only be 15, 16 months since last we saw him. I hope that when he comes, it is not another hurried appearance, where those of us at the end of the table are told he has to be off to a noon meeting. That has happened before, and I hope it does not happen again.

I would like to ask if—

Chairman HATCH. Just so the record is clear, he was going to come at the end of March or in March, but then he got very sick—

Senator DURBIN. I am perfectly aware of the medical problems he faced.

Chairman HATCH. We will get him in here.

Senator DURBIN. It will be great to see him. It has been a long time.

Let me ask you this, Director Mueller. Can you clarify something about Nicholas Berg? I am troubled by the press reports that have been out about him, and what a tragedy that this would happen to any person and be publicized in a fashion so that the world and his family would know these barbaric circumstances that led to his death. It should be condemned by everyone.

But tell me about this man. Was he detained in Iraq when he tried to leave because he was under investigation or there was some suspicion he had done something wrong?

Mr. MUELLER. My understanding is that he had been detained by Iraqi police officers. The circumstances under which they detained him, I am not sure are totally clear. He was detained. He came to our attention. We did an indices check and determined that he had had some tangential association with Moussaoui, whom I believe you know was arrested shortly before September 11th, which warranted us doing follow-up interviews. And we did follow-up interviews with Mr. Berg, found that he had, as far as we were concerned, no association with terrorism. He was then released.

At the time of his release, he was spoken to by, I believe, individuals of the CPA, and I believe our agents as well, who urged him to leave. And my understanding is that CPA also indicated that if he did not have the wherewithal to leave, they would supply it to him. He turned them down, went to a hotel. I also believe that there was a request made by CPA authorities that they be able to alert his family, and my understanding, and I would have to check on this, is that he declined that that be done, and then he became missing from his hotel. It is indeed a tragedy, but those are the circumstances, to the best of my knowledge.

Senator DURBIN. Well, and of course it has been publicized that his family went to Federal Court in Philadelphia, if I am not mistaken, trying to force his release from detention so that he could leave the country. So it appears that there is some conflict as to his intentions and what actually occurred.

But I think you have made it clear for the record, and I hope it is unequivocal, that there has never been any suspicion of any wrongdoing or illegal activity on his part.

Mr. MUELLER. No. As I said before, he was a person we interviewed in the wake of September 11th, and the interview indicated that he was not associated in any way with terrorists, and that was again confirmed when we interviewed him in Iraq.

Senator DURBIN. Was he at any time working with a U.S. agency for intelligence or any agency that you are aware of to try to gather intelligence?

Mr. MUELLER. Not to my knowledge. My understanding was he was in Iraq to try to develop his own private business that was related to cell phone towers, I believe.

Senator DURBIN. Those are the press reports. And I also would like to switch, if I could, to an issue that has been discussed over and over here, and that is the PATRIOT Act, which I voted for and most members did, but I am also co-sponsoring with Senator Craig the SAFE Act not in an attempt to eliminate the PATRIOT Act, but rather, in specific instances, to require what we consider to be necessary safeguards within that Act.

I will concede that a lot of work went into it, but I think most Senators will agree that an act of this historic moment moved through in record time. It was in light of our concern about the threat of terrorism. We tried to be responsive. We put in a safeguard to say that we would revisit some of these issues. We put sunsets on the provisions to make sure that they were wise in their conception and being used in a fair and judicious fashion.

I am concerned, though, as I look at the provisions in the act, that we have just made some statements here at the hearing that I do not think accurately reflect the changes in the law that are included in this PATRIOT Act. This Section 213, the delayed notification, sneak-and-peek, depending on your personal feelings on this, clearly puts a standard of reasonable period into the law as to how long you can proceed without notification.

The court cases, as you are well aware, said 7 days, and after 7 days, at that point, the Government has a burden to come forward and explain why they are delaying the notification. But this provision, and this is in existing law—the 7-day notification—but in the PATRIOT Act what we are dealing with here is virtually indefinite in terms of notification.

What we have tried to do—what Senator Craig and I have tried to do—is to provide specific exceptions for circumstances that have been described here. We have said that we would continue to delay notification of a warrant if there was any possibility that notification would endanger a life or physical safety, result in flight from prosecution or a destruction of or tampering with evidence. Now, I think that creates a reasonable model, a reasonable standard, which says that if you cannot establish one of those elements, then at some point notification must be given.

What exception do you think we have missed here in this providing for notification that you think would somehow jeopardize your work?

Mr. MUELLER. Well, every investigation is different. There are some investigations where delay of, yes, 24 hours would be sufficient. There are some investigations where delays of 30 or 60 days might be entirely appropriate if it is a large investigation. What the PATRIOT Act, I think, appropriately does is leave the duration up to the judge to decide on the facts that are presented when the judge issues the order, and I have not found judges reluctant to act and set parameters based on what the prosecutors and the agents show them.

In terms of the changes to the PATRIOT Act that is proposed by the SAFE Act, the elimination of "seriously jeopardizing an investigation", I think, would adversely affect our ability to set a set of

circumstances before a judge which shows that the delay is necessitated by the unique circumstances of investigation.

What I believe the SAFE Act does is leave in some more narrowly defined bases for obtaining the delayed notification, but there are a number of circumstances that come up in an investigation which I don't think you can necessarily cubby-hole, but that a judge looking at it can say, okay, this is going to seriously jeopardize an investigation, and therefore I ought to delay the notification for 60 or 90 days.

Senator DURBIN. Director, I think that, though I may not agree with the specific language, I think that is a good-faith suggestion.

Mr. Chairman, you have suggested a hearing on the SAFE Act, and when we get into it, I think, if we are going to try to establish standards that meet your goals and ours, we are I think going to tighten it without eliminating the expansion of Government authority to go after terrorism. I would like to work with the Chairman and the Director to come up with that language. I think that is important, and maybe we can reach that goal. I hope that we can in the course of what we are setting out to do.

I would also just like to make one comment before I close, and you have been very patient, Mr. Director, as has the Chairman, waiting for those of us in lowly status to have our moment, but let me just say that many have said here we just have not heard any complaints about this PATRIOT Act. Well, I do not think that that is an appropriate standard when it comes to protecting our freedoms in this country. Much of the work being done under the PATRIOT Act will be done without the knowledge of the person who may be having their rights violated, and so they may not even have knowledge that this is going on when they are the subject of investigations or wiretaps or searches under the PATRIOT Act.

So I would hope that we can still establish, as a standard, that there are very, very efficient ways for this Government to collect information which clearly violate the Constitution, and we have to find a way to draw a line to preserve security in this society while still maintaining our mutual oath to uphold the Constitution.

Chairman HATCH. Thank you, Senator. Your time is up.

I have not used my time, nor do I intend to, but let me just say that I think the PATRIOT Act is one of the most misunderstood acts of legislation I have ever seen. The media, and the public, and many of the pundits have focused on hypothetical abuses. But as my dear friend from California, Senator Feinstein, has mentioned at a prior hearing, not even the ACLU has been able to cite a single instance of actual abuse, and they watch things very carefully, and I commend them for doing so because they serve this country well when they do that.

I held a Senate hearing in Utah in April, and we invited a plethora of critics of the PATRIOT Act, yet not one single one of them could cite even one example of actual abuse, not the ACLU, not the League of Women Voters, not the Conservative Caucus, not the Eagle Forum, not the Libertarian Party. They were all there. They were all hypothetical: Oh, what if—what if this happened or that happened.

But my big "what if" is what if we do not have the tools to prevent terrorism in this country in the future? That is why the PA-

TRIOT Act is so important. Now, we will have further hearings on this, and I do intend to have a hearing on the SAFE Act. I think my colleagues feel that that is something that should be done, and Senator Leahy and I will hold that hearing.

But I just want to thank you. I know you have got to go, and I know we have kept you beyond the 1 o'clock time that I said I would try to keep it in, and I have appreciated your patience and your kindness in spending this amount of time with us, and it has been very beneficial and fruitful for the Committee and I think for the public at large who may see this on C–SPAN.

With that, then, Senator?

Senator LEAHY. I also want to join with you, Mr. Chairman, in doing that and thanking the Director. He has been here. He has answered a whole lot of questions. This has been a good hearing. Normally, in the role of Ranking Member, I could ask my questions and leave. I have stayed here for it because I found the answers and the questions, on both sides of the aisle, to be very informative, very worthwhile. I appreciate the information.

I might just add a personal point of view. I know you quite well, I believe. You are former law enforcement, former Marine. I can imagine you felt like a former Marine who is near and dear to me, how he felt when he saw the pictures of the prisoners. And I think, as I am sure you do, the 138,000 American men and women over there in the uniform who are carrying out their duties every day, doing exactly what they should do and put in increased danger, to say nothing about your own agents, and contractors.

So I thank you for being here. And, Mr. Chairman, I thank you, and I applaud you for this hearing.

Chairman HATCH. Well, thank you. And I just want to thank the FBI. The American people need to know the tremendous job that you folks are doing for our country. I mean, you are just under pressure all of the time. Most of the agents are underpaid for the risks they take and the pain that they go through for all of us.

I know that a person like you could go out into the private sector and make a fortune, but you have chosen to serve in public service, and sometimes you have to take abuse for doing that, that you really should not have had to take. And to be honest with you, I have really appreciated you being here today, and I appreciate the service that you are giving.

Now, I will keep the record open for any written questions that any member of the Committee would care to send, and I hope that you and your staff will answer those as soon as possible.

Mr. MUELLER. Thank you, Mr. Chairman.

Chairman HATCH. Just do not let anybody believe for a second that our FBI is not doing the very best it can, and I do not know where we would be without folks like you and the good public servants who serve us through the FBI.

Thank you for the time. Sorry to keep you so long.

Mr. MUELLER. Thank you.

Chairman HATCH. With that, we will recess until further notice.

[Whereupon, at 1:28 p.m., the Committee was adjourned.]

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

QUESTIONS AND ANSWERS

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 1, 2005

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

Dear Mr. Chairman:

Enclosed please find responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on May 20, 2004. The subject of the Committee's hearing was "FBI Oversight: Terrorism and Other Topics."

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

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Responses of the Federal Bureau of Investigation
Based Upon the May 20, 2004 Hearing Before the
Senate Committee on the Judiciary
Regarding "FBI Oversight: Terrorism and Other Topics"

Questions Posed by Senator Hatch

1. In order to more fully understand this issue, please provide a chronology of events leading up to the misidentification of Mr. Mayfield. Include in this chronology an explanation of the events leading up to the initial identification of Brandon Mayfield as well as the circumstances that led to acknowledgement that Mayfield had been misidentified. Specifically, what efforts were made to secure the original or best fingerprint evidence? How many requests were made? Was there any attempt to utilize the actual prints held by the authorities in Spain? How many visits to Spain were made regarding the fingerprints in question? When was Mr. Mayfield officially identified? At what point did the FBI become aware of the doubts of the Spaniards as to Mr. Mayfield being the owner of the prints in question? When did the FBI discover the misidentification? What actions were taken immediately following the misidentification?

Response:

The FBI provided two briefings to Committee staff concerning this issue; first on 5/25/04 and again on 6/9/04. Since that time, both the Department of Justice (DOJ) Office of the Inspector General (OIG) and the DOJ Office of Professional Responsibility (OPR) have initiated separate reviews of the Mayfield matter. The FBI will cooperate fully with these reviews and looks forward to the forthcoming reports from OIG and OPR. In addition, Brandon Mayfield has filed a lawsuit against the FBI, DOJ, and certain individuals arising out of this matter. In light of the pendency of the OIG and OPR reviews and the Mayfield lawsuit, it would be inappropriate to provide additional comment at this time.

2. a. Please describe the standard protocols and methodologies that FBI fingerprint examiners use to determine whether a particular latent fingerprint is of value for identification purposes and whether such protocols and methodologies were utilized in the case of Brandon Mayfield.

b. What is standard procedure regarding the use of direct evidence versus secondary evidence?

c. In addition, what changes, in policy and procedure, do you anticipate making in order to assure the American public that such misidentification and wrongful incarceration does not happen again?

Response to a through c:

As indicated above, the FBI will defer response during the pendency of the OIG and OPR reviews and the Mayfield lawsuit.

Questions Posed by Senator Grassley

3. The Department of Justice recently released a report regarding the FBI's analysis of alternative financing mechanisms in money laundering and terrorist financing cases. The report, which is a 3 page document, states that TFOS has established a Program Management and Coordination Unit to analyze data on alternative financing mechanisms.

a. Thus far, what trends have been found regarding alternative financing mechanisms?

Response:

The response to this question is provided For Official Use Only (FOUO), and is included with the classified response.

b. How is the information being utilized to initiate other terrorist financing investigations?

Response:

The data from the field survey discussed above will be used to develop and enhance an analytic framework based upon identifiable patterns and trends. The analytic framework will enable Joint Terrorism Task Forces (JTTFs) to identify potential terrorism connections in investigations and facilitate the identification of previously unknown or "sleeper" terrorist suspects. In the interim, all pertinent information and data will be disseminated to the JTTFs and other agencies and entities as appropriate.

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

Response:

The FBI has pursued more than 400 investigations concerning terrorism financing since 9/11/01. Unfortunately, because the vast majority of these investigations are ongoing, the FBI is unable to provide this information to the Committee at this time. (The very small number of cases that have been closed typically are offshoots of more significant ongoing investigations or involve very narrow facts, and do not reflect the nature, complexity, or value of the ongoing investigations.) The FBI would be pleased to provide this information to the Committee through classified briefings or other appropriate vehicles once the investigations have been closed.

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

Response:

Information sharing is critical to the efforts of the United States Government (USG) against terrorism and criminal activities. The United States Intelligence Community (IC), including the FBI, produces and obtains tremendous amounts of classified intelligence information. While much of the information can be of significant value in terrorist finance investigations, this value may not be realized or maximized without the ability to filter, analyze, and disseminate the information to those who can make the best use of it.

The data analysis will be available to appropriate investigative, regulatory, and intelligence agencies through the JTTFs. TFOS also participates in joint endeavors with the Treasury Department, others in DOJ, and the Department of Homeland Security (DHS) with respect to potential terrorist-related financial transactions and money laundering.

In addition, the National Security Council (NSC) established the Policy Coordinating Committee (PCC) on Terrorist Financing at the end of 2001. The NSC chairs the PCC, which generally meets at least monthly to coordinate the USG's campaign against terrorist financing. The FBI presents all pertinent information at the PCC meetings, which focus on ensuring that all relevant components of the federal government are acting in a coordinated and effective manner to combat terrorist financing.

4. Recently, the National Research Council, at the FBI's request, reviewed the Trilogy program and found the system inadequate for counter-terrorism analysis and significantly over budget. The Council recommended that the FBI scrap the whole thing and start over.

a. Are you following the Council's recommendations regarding testing and implementation?

Response:

Yes. A 5/10/04 report by the National Research Council identified five areas of focus, and a 6/7/04 letter by the National Academies Chair of the Committee on the FBI's Trilogy modernization program advises that the FBI is addressing all five areas consistent with the Council's recommendations by: 1) converting from the Automated Case Support (ACS) system to a more powerful, user-friendly system, 2) creating an Enterprise Architecture (EA), 3) developing linked enterprise subarchitectures, 4) restructuring the Trilogy management plan, and 5) increasing internal FBI expertise in information technology (IT) and contract management.

b. How will the additional funding you requested address the basic concerns that the system does not work?

Response:

The FBI has completed two of the three components that comprise the Trilogy program. The Transportation Network Component and the Information Presentation Component were completed, providing the FBI with the Trilogy infrastructure, including the installation of the LAN, WAN, workstations, printers, and scanners in all Field Offices, resident agencies, offsites, and FBI Headquarters. Trilogy has also provided the FBI with Full Site Capability, which included the installation of new servers, upgrading of the FBI's office automation and learning management systems, and the provision of Microsoft Outlook email for all FBI users. The User Application Component is the only piece of Trilogy that has not yet been completed.

Although the FBI received funding in FY 2004 for Trilogy Operations and Maintenance and technical refreshment, it has not received any additional funding for Trilogy development since the Trilogy reprogramming in FY 2003. As indicated in response to Question 4a, above, the FBI's IT modernization program is ongoing. Included in the modernization program is the completion of a software application that will improve the FBI's efficiency, workflow, and records management functions.

c. What solution do you recommend for ensuring that the FBI has an adequate computer system to support its intelligence and analytical needs?

Response:

An Office of Intelligence (OI) Executive Working Group, chaired by OI and facilitated by the Office of the Chief Information Officer (OCIO), was created to identify the enterprise IT requirements needed to support OI operations. Participants in the working group include representatives from operational and support Divisions at FBI Headquarters (FBIHQ) as well as FBI Field Offices. The initial focus of the working group is the identification of immediate and near-term IT requirements; "requirements" are defined as the high-level, end-goal business and mission operational needs to support FBI intelligence activities.

Initial analysis of the immediate and near-term OI IT needs, which are those that can be addressed within 6 to 12 months, resulted in the identification of 53 "requirements." The 53 requirements have been validated and provided to the OCIO for systems/solution development.

Collection of the mid-term IT requirements, which are those that can be completed within 1–3 years, has been initiated.

5. Drug trafficking is one of the main industrial and financial bases for the funding [of] terrorism and terrorist organizations. In Afghanistan, for example, the explosion of opium production poses a significant threat to our ability to halt terrorist financing in that region. What action is the FBI currently taking to address the direct connection between terrorism and drug trafficking in that country, as well as other countries such as Colombia that have a significant drug/terror nexus?

Response:

Through the JTTFs, TFOS has partnered with investigative, regulatory, and intelligence agencies to determine the genesis of funding to terrorist groups. The FBI continues to gather intelligence and actively investigate all leads with respect to drug trafficking as a source of such terrorism funding.

Historically, Afghanistan has been a major source of heroin throughout the world. While conventional wisdom and some press accounts support the premise of the question, exhaustive investigation has not revealed direct evidence that drug trafficking proceeds support extremist groups. This does not mean there is no basis for inferring a likely link. For example, a joint FBI/DEA investigation in 2003 resulted in the arrests of 16 Afghan and Pakistani subjects for involvement in an extensive drug ring. The investigation revealed that heroin, grown and processed in Afghanistan and Pakistan, was being shipped to the United States. Profits from the sale of the heroin were laundered through Afghan and Pakistani-owned businesses and then sent back to suspected associates of terrorist organizations. A direct link between the drug trafficking profits and terrorist organizations was, however, not proven.

With respect to Colombia, the FBI is aware that the region continues to produce and distribute cocaine and is a significant supplier of heroin to the United States. In addition to supporting independent drug traffickers and cartels, the drug trade serves as a major source of funding for the Revolutionary Armed Forces of Colombia (FARC) and the United Self Defense Forces of Colombia (AUC). The AUC and FARC each control areas within Colombia that support coca and poppy cultivation. FBI investigations have led to the prosecution of both members and leaders of these organizations.

6. It is my understanding that the FBI is implementing the National Security Support Capability (NSSC) program. The NSSC will be an important tool in the FBI's arsenal in the war on terrorism, because it brings a highly valuable new mix of methods and approach to this highest priority problem. There is considerable support for this unique effort on both sides of the Capitol and both sides of the aisle. I am pleased that you have included it in your FY06 budget and your program plans. But 2006 is too far off.

a. Could you tell me what efforts you are taking to implement the program now?

Response:

The FBI's CTD has recently held a series of meetings with DHS and the Department of Energy (DOE) concerning the National Security Support Capability (NSSC). Based on these meetings, CTD developed a plan to incorporate the NSSC into its training mission and to work with private industry beginning in 2005. In August 2004, CTD and DOE worked out an arrangement to detail a DOE employee to the FBI for one year to assist in initiating this program. Later that same month, the DOE detailee unexpectedly withdrew from the detail assignment and is no longer supporting the NSSC initiative.

CTD and DHS have discussed alternative solutions that will deliver results that are the same as or similar to those expected from the NSSC. These discussions are ongoing but are too formative to permit comment on specific programs or dates of delivery.

b. Using this program first on threats and vulnerabilities to the U.S. food supply is a great beginning and will bring an enthusiastic response from those of us who know how important it is to protect this critical resource. What other priorities will the program be extended to?

Response:

Discussions regarding the NSSC's scope have indicated that it can be applied not only to the food and agriculture industries, but to a range of industries, including telecommunications and the oil and gas industry. Current discussions with DHS include focus on the possible uses of this or similar methodologies to produce valuable security-related information.

Questions Posed by Senator Leahy

Prisoner Abuse

7. I asked you at the hearing how many FBI agents were currently stationed in Iraq, Afghanistan, and Guantanamo Bay. You offered to submit that information for the classified record. Please do so now. In addition, please state how long these agents have been stationed in these countries, and describe their mission(s).

Response:

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

8. At the hearing on May 20, you stated that the Department of Defense had not, to date, referred any prisoner abuse cases involving military contractors to DOJ. The next day, DOJ announced that it had received such a referral the day before and that it had "opened an investigation into the matter."

a. At what time on May 20 did DOJ receive the referral from DOD?

Response:

The referral described was initially directed to an attorney in the Department's Criminal Division who had been previously identified to the Department of Defense as a point-of-contact for matters of this sort. The attorney learned of the referral in the middle of the day on May 20. At the time of the hearing, the FBI had not yet been informed of the referral.

b. When did you first learn about that referral?

Response:

The FBI learned about the referral close in time to when the information was publicly released, approximately May 21.

c. Is the FBI conducting this investigation and, if not, what investigating body is?

Response:

It is the FBI's understanding that the investigations into prisoner abuse by civilians were referred to the U.S. Attorney for the Eastern District of Virginia. Investigative materials have been provided to the FBI and the FBI is currently evaluating them.

9. At the hearing, you noted that the CIA had referred a prisoner abuse case to DOJ, but that the investigation was being conducted by the CIA Inspector General and not the FBI. Has the FBI become involved in that investigation since the hearing? If not, what investigating body or bodies are involved?

Response:

One case involving prisoner abuse was referred to the FBI by the CIA Inspector General and the FBI has opened an investigation into that allegation.

10. At the hearing, I asked you whether any of your agents have encountered any objectionable practices involving the treatment of prisoners in Iraq, Afghanistan or Guantanamo Bay. You limited your answer to Abu Ghraib, stating that none of your agents had witnessed abuses in that facility. Subsequently, in response to a similar question by Senator Feinstein, you stated, "We have, upon occasion, seen an area where we may disagree with the handling of a particular interview. And where we have ... seen that, we have brought it to the attention of the authorities who were responsible for that particular individual."

a. Upon how many occasions since September 11, 2001, have FBI agents "disagreed with" the handling of a prisoner interview in Iraq, Afghanistan, or Guantanamo Bay?

b. In how many of these cases was such disagreement "brought to the attention of" the responsible authorities?

c. What authorities were notified of the FBI's "disagreement" with particular interviews, and what, if anything, did they do in response? Did the FBI ever follow up with these authorities to determine if its concerns had been addressed?

d. What was the FBI's role in these interviews? Were agents actively involved and asking questions, or were they merely observing?

e. What sorts of practices did FBI agents "disagree with"? Please provide specific examples.

f. What guidance have field agents received from HQ about how to proceed in the event of a "disagreement" with another agency's handling of prisoner interviews?

g. Please provide copies of any written reports generated since September 11, 2001, that note an FBI agent's "disagreement" with, or objection to, the handling of a prisoner by the CIA, DOD, or any other American entity, in Iraq, Afghanistan, or Guantanamo Bay.

Response to a through g:

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

There are, however, other schools of thought regarding the best means of obtaining information from recalcitrant individuals. These varying schools of thought were at the heart of the disagreement over which interrogation methods should be used against individuals captured and suspected of involvement in terrorism against the United States.

In 2002, as a matter of policy, the Director of the FBI determined that, regardless of the legality of more aggressive interrogation techniques, FBI personnel would not participate in interrogation techniques that would not be appropriate for use within the United States. Rather, they would at all times conduct interrogation in accordance with FBI policies. A 5/19/04 electronic communication reiterating this policy, and directing FBI employees to report known or suspected abuse or mistreatment of detainees, follows this response.

Prior to the Committee's 5/20/04 hearing, the FBI surveyed its employees who were at Abu Ghraib prison during the time period of abuse as identified in General Taguba's report. That survey revealed no knowledge by FBI employees of the sort of abuses that were publicized around the time of the hearing. FBI employees were aware, however, of detainees being subjected to sleep deprivation and environmentally harsh conditions. The results of that survey were provided to the Department of Defense (DOD) for such follow-up as it deemed appropriate.

During 2002, there were disagreements in Guantanamo between the FBI and DOD concerning the interrogation plan that would be used for a particular detainee, and more general disagreements regarding the efficacy of rapport building techniques as opposed to more aggressive interrogation techniques. A classified electronic communication dated 5/30/03 documents these discussions and is provided under separate cover.

Subsequent to the Director's testimony before the Judiciary Committee, the FBI surveyed its personnel who had been in Guantanamo to determine whether any witnessed mistreatment of detainees. Prior to that survey, three incidents in which FBI personnel witnessed questionable treatment of detainees had been orally discussed with members of the DOD Office of General Counsel, in early 2003. Follow-up correspondence to Major General Donald J. Ryder, Department

of Army Criminal Investigation Command, dated 7/14/04, is provided separately.

The Guantanamo survey revealed other instances of treatment of detainees by non-FBI employees that would not have been in accord with FBI policy. All responses to the survey that included any knowledge of such treatment of detainees have been communicated to DOD for such follow-up as it deemed appropriate.

The FBI has not surveyed all Agents who have served in Afghanistan as to their knowledge of aggressive techniques. Some Agents have expressed concerns as to techniques being utilized in Afghanistan by non-FBI personnel. That information is being provided to DOD officials. In addition, the DOJ OIG has initiated an investigation into alleged abuse of detainees at Abu Ghraib, Guantanamo, Afghanistan, and any other venue controlled by the U.S. military. We are cooperating and providing relevant information in conjunction with the OIG inquiry as well.

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 05/19/2004

To: All Divisions

Attn: ADIC
AD
DAD
SAC
CDC

From: General Counsel
Contact: Donald Klein (202) 324-0605

Approved By: Pistole John S
Caproni Valerie E

Drafted By: Klein Donald J
Matsumoto Lisa K

Case ID #: (U) 66F-HQ-A1258990

Title: (U) Treatment of Prisoners and Detainees

Synopsis: (U) In light of the widely publicized abuses at the Abu Ghraib prison, Iraq, this EC reiterates and memorializes existing FBI policy with regard to the interrogation of prisoners, detainees, or persons under United States control (collectively "detainees"). These guidelines serve as a reminder of existing FBI policy that has consistently provided that FBI personnel may not obtain statements during interrogations by the use of force, threats, physical abuse, threats of such abuse or severe physical conditions. In addition, this EC sets forth reporting requirements for known or suspected abuse or mistreatment of detainees.

Details: (U) FBI personnel posted abroad come into contact with detainees in a variety of situations. Persons being detained or otherwise held in the custody of the United States are entitled to varying levels of procedural rights depending upon their situation or category of detention (*e.g.*, unlawful combatant, prisoner of war). Although procedural rights, such as Miranda rights, do not apply in all situations overseas, certain minimum standards of treatment apply in all cases.

Applicability: (U) FBI personnel and personnel under FBI supervision deployed in Iraq, Guantanamo Bay, Cuba, Afghanistan or any other foreign location where similar detention and interrogation issues arise are to follow FBI policies and guidelines for the treatment of detainees.

FBI Policy: (U) "It is the policy of the FBI that no attempt be made to obtain a statement by force, threats, or promises." FBI Legal Handbook for Special Agents, 7-2.1 (1997). A person's status determines the type and extent of due process rights accorded by the FBI, such as right to counsel or advisement of rights. Regardless of status, all persons interrogated or interviewed by FBI personnel must be treated in accordance with FBI policy at all times. It is the policy of the FBI that no interrogation of detainees, regardless of status, shall be conducted using methods which could be interpreted as inherently coercive, such as physical abuse or the threat of such abuse to the person being interrogated or to any third party, or imposing severe physical conditions. *See*, FBI Legal Handbook Section 7-2.2.

Joint Custody or Interrogation: (U) FBI personnel who participate in interrogations with non-FBI personnel or who participate in interrogations of persons detained jointly by FBI and non-FBI agencies or entities shall at all times comply with FBI policy for the treatment of persons detained. **FBI personnel shall not participate in any treatment or use any interrogation technique that is in violation of these guidelines regardless of whether the co-interrogator is in compliance with his or her own guidelines**. If a co-interrogator is complying with the rules of his or her agency, but is not in compliance with FBI rules, FBI personnel may not participate in the interrogation and must remove themselves from the situation.

Reporting of Violations: (U) If an FBI employee knows or suspects non-FBI personnel has abused or is abusing or mistreating a detainee, the FBI employee must report the incident to the FBI on-scene commander, who shall report the situation to the appropriate FBI headquarters chain of command. FBI Headquarters is responsible for further follow up with the other party.

To: All Field Offices From: General Counsel
Re: (U) 66F-HQ-A1258990, 05/19/2004

LEADS:

Set Lead 1 (INFO)

ALL RECEIVING OFFICES

(U) Distribute to all personnel.

Set Lead 2 (INFO)

COUNTERTERRORISM

AT WASHINGTON, DC

(U) To be distributed to all FBI personnel who are now, or in the future are, detailed to Iraq, Guantanamo Bay, Cuba, or Afghanistan or other foreign locations in which similar detention and interrogation issues may arise.

♦♦

11. Do you think it is appropriate for the U.S. to use interrogation methods that are prohibited under U.S. law, as well as by the Geneva Conventions, to gain information in terrorism investigations? Has the FBI used any information produced by such methods in any terrorism case it is investigating or prosecuting?

Response:

I do not believe it is appropriate for the United States to use interrogation methods that are unlawful under applicable law. It is FBI policy that all interrogations, regardless of the status of the person being interrogated, shall be conducted using methods that would be lawful if used within the United States (except that Miranda warnings are not required prior to extraterritorial questioning conducted for intelligence purposes). Among the techniques that FBI employees may not use, therefore, regardless of whether the interviewee is a U.S. citizen or an unlawful combatant taken into custody on the battlefield of Afghanistan, are physical abuse, the threat of such abuse to the person being interrogated or to any third party, or the imposition of severe physical or environmental conditions.

Nicholas Berg

12. There is continuing confusion as to who held Nicholas Berg in custody and for how long. The Iraqi police deny ever holding Mr. Berg, and Mr. Berg's father has asserted that he was held illegally by the U.S. for two weeks. You testified, in response to a question from Senator Durbin, that Mr. Berg was detained by Iraqi police officers under circumstances that "I am not sure are totally clear"; Mr. Berg then "came to our [the FBI's] attention"; the FBI did some follow-up interviews with Mr. Berg and found that he had no association with terrorism, whereupon Mr. Berg was released and urged to leave Iraq.

a. Did the U.S. Government ever hold Mr. Berg in U.S. custody for any period of time?

Response:

The FBI did not have Mr. Berg in custody. Mr. Berg was interviewed by FBI personnel at the One West Iraqi Police Station in Mosul, Iraq, on 3/25/04, 3/26/04, and 4/3/04.

b. Did the U.S. Government ever ask or encourage the Iraqi police to arrest or detain Mr. Berg?

Response:

Mr. Berg was detained by the Iraqi Police on 3/25/04 without the knowledge of the FBI. The FBI was notified of Mr. Berg's detention later that day.

Following his detention by Iraqi police, FBI personnel were asked to evaluate Mr. Berg for security purposes. After interviewing Mr. Berg and conducting preliminary background checks, FBI personnel expressed an investigative interest in Mr. Berg. It was understood that Mr. Berg would not be released until a more thorough investigation was completed and any security issues involving him were resolved.

c. Did the U.S. Government ever make any efforts on behalf of this citizen, to secure his release from custody?

Response:

Yes. The FBI interviewed Mr. Berg several times, conducted background checks, and followed up on leads in the U.S. relating to Mr. Berg. Once these steps were completed, the FBI advised the U.S. military and the Coalition Provisional Authority (CPA) that the FBI had no investigative interest in Mr. Berg.

d. Has the U.S. Government ever inquired into the circumstances under which Mr. Berg was arrested and detained? If so, please describe those circumstances with specificity. If not, why not?

Response:

The FBI was informed by the CPA that Mr. Berg had been detained by Iraqi Police while riding in a taxi in Mosul, Iraq. Because of the high level of violence in that area, the Iraqi Police were on the lookout for suspicious activity and for any individuals who did not appear to be from the area. In an interview, Mr. Berg disclosed that he had been arrested previously by Iraqi Police in January 2004 in Diwaniya, Iraq, because he looked suspicious.

Brandon Mayfield

13. On Monday, May 24, a federal court dismissed the material witness proceeding against Oregon lawyer and former army officer Brandon Mayfield, and the FBI expressed regret for the erroneous fingerprint match that led to his arrest. The FBI has said that it made the initial match by running a latent fingerprint from the Madrid train bombing investigation through the Integrated Automated Fingerprint Identification System (IAFIS).

a. Did the FBI run the latent print against the entire IAFIS database, or against some sub-database of IAFIS that has been created for terrorism investigations? If the latter, please explain how Mr. Mayfield's print came to be included in the terrorism database.

b. The FBI has said that IAFIS produced 20 possible "hits" with the latent print from the bombing, the fourth of which belonged to Mayfield. To whom did the other 19 prints belong? As to each of these 19 individuals, how did his or her fingerprints come to be included in IAFIS?

c. What, if any, additional information was provided to the investigators and/or the lab technicians by IAFIS and/or the Criminal Justice Information Services (CJIS) Division at the time the 20 fingerprint cards (the "hits") were sent to the laboratory for a side by side comparison?

d. The FBI has maintained that its lab technicians had no idea who Mayfield was when they matched his fingerprint to the latent print from the bombing investigation. It does seem improbable that the match happened to be with a Muslim lawyer who once represented the chief defendant in the "Portland Seven" terror case. What steps have been taken by the OIG or the FBI to review the actions of those responsible for this mismatch?

e. I understand that the FBI was able, ultimately, to review the best evidence of the questioned latent print in order to eliminate Mr. Mayfield as the suspect, but did not review that evidence to determine whether the "points of identification" that had been made were, in fact, erroneous as well. Does the FBI intend to conduct such a review to determine what, if any, errors were made in that portion of the original analysis? If not, why not?

f. What statements were made to the court by any government representative, at any time, orally or in writing, about the fingerprint "match"?

g. Please provide a copy of the original fingerprint report prepared by the examiner.

h. Following the erroneous fingerprint match, was Mayfield the subject or target of any secret surveillance under FISA or any other national security authority? Please explain your answer.

i. Was the fingerprint that was originally identified as Mayfield's the very same fingerprint that was ultimately identified by the Spanish authorities as belonging to a suspect from Algeria? If it was a different fingerprint, were the two fingerprints (the one misidentified as Mayfield's; the others belonging to the Algerian man) on the same, or a different, piece of evidence? Please describe the pieces of evidence on which the fingerprints were identified. How many fingerprints have the Spanish authorities identified as belonging to the Algerian and on what pieces of evidence?

Response to a through i:

As indicated above, the FBI will defer response during the pendency of the OIG and OPR reviews and the Mayfield lawsuit.

Fingerprint System

14. Earlier this year, Inspector General Fine issued a report on the slow pace of the integration of IDENT and IAFIS, the fingerprint identification databases of the former INS and the FBI. The report examined the case of Victor Manual Batres, a Mexican national with a criminal history who was twice simply returned to Mexico by Border Patrol agents whose database did not identify him as a wanted man. Batres eventually entered the country illegally, and then raped two nuns in Oregon, killing one. The Inspector General reported that the integration that would give Border Patrol agents access to the FBI database was two years behind schedule, and was not expected to be completed until 2008. This report is the third OIG report in the last four years to highlight various aspects of this problem.

a. Why has progress on this issue been so slow?

Response:

During 1990 and 1991, the FBI and the Immigration and Naturalization Service (INS) met to discuss possible coordination of their planned automated fingerprint identification systems. Memoranda summarizing some of these meetings indicate that the INS and FBI were attempting to determine if an integrated fingerprint system could satisfy INS's needs. The memoranda also include preliminary diagrams and narratives as to how the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the INS's proposed system (which evolved to become the Automated Biometric Identification System (IDENT) system) could be linked in an overall automated fingerprint identification system network. There was also discussion of how to ensure common high-quality fingerprint image and electronic transmission standards for fingerprints and identification data so that they could be transmitted among different fingerprint identification systems.

The INS and FBI recognized that integration of their separate automated fingerprint identification systems would benefit both agencies. An integrated system would reduce the likelihood that INS would release an alien who had a serious criminal record and prior deportations. It also would enable federal, state, and local law enforcement authorities to search fingerprints from a crime scene against an immigration database of those who have crossed borders illegally.

The two identification systems are, however, not yet interoperable. This is in part because each system was designed to meet different mission requirements: IAFIS was designed to match ten-print submissions against a ten-print database because this is the best means by which law enforcement can identify criminal subjects (since crime scenes may offer latent prints from any of a subject's ten fingers), and IDENT was developed with a two-print standard in order to meet the need to quickly and accurately verify an individual's identity.

DOJ and DHS have undertaken an effort to integrate the FBI's IAFIS with DHS's IDENT. This multi-year effort is designed to give DHS the ability to determine quickly whether an individual, such as a person encountered at a border crossing, has a record in the criminal master file of the FBI's IAFIS. Full integration would also enable other law enforcement agencies to obtain an individual's DHS apprehension history through the IAFIS infrastructure and communications network. DOJ and DHS continue to research possible solutions. The FBI will continue to provide support to DOJ by providing relevant information concerning operational impacts on the FBI.

b. When can we expect that the databases will be integrated?

Response:

An initial phase of integration has occurred with the deployment of integrated IDENT/IAFIS workstations at ports of entry across the United States. Completion of the integration process depends on the development of appropriate interoperability standards. DHS and DOJ are working together to resolve these issues as expeditiously as possible in the pursuit of full integration.

Trilogy

15. The Trilogy project is now more than $200 million over budget and still incomplete.

a. Is the FBI cooperating fully with the OIG's audit of the cost and contractual issues involved?

Response:

The FBI cooperated fully with DOJ's OIG, providing that office with extensive documentation relative to the Trilogy audit.

b. Can you assure me that the FBI will cooperate fully with a subsequent review that Senators Hatch, Grassley, Durbin and I asked the GAO to complete regarding fraud, waste and abuse?

Response:

The FBI has cooperated, and will continue to cooperate, fully with GAO reviews requested by Congress.

c. Has the FBI done any investigation of its own into whether there has been any fraud, waste or abuse involved in this government contract?

Response:

A financial review of the Trilogy funding was conducted by the FBI Inspection Division's Audit Unit during January and February 2004. The objectives of the review were to determine: 1) the overall funding used in support of Trilogy; 2) what funds remain available to support the Trilogy roll out; 3) whether transactions where recorded accurately within the financial management system; and 4) whether the program had adequate financial management oversight.

The financial review identified some compliance deficiencies and internal control weaknesses, the most prominent of which was the inability to obtain a global financial profile. The FBI has taken action to resolve the deficiencies and internal control weakness identified through this review.

16. Please provide me a detailed chronology of the key contractual events for all parts of Trilogy.

Response:

The enclosed memorandum dated 1/26/05 contains an historical account of the FBI Trilogy effort.

The Trilogy contract with Dyncorp/CSC for the hardware and software components was completed in April 2004.

17. You testified that "the reason we have spent far more funds" on Trilogy is that the contracts for the program were entered into in the summer of 2001, and the program had to be "changed and adapted" in the wake of the 9/11 attacks. Please specify what changes/adaptations were made to Trilogy as a result of the 9/11 attacks that account for the more than $200 million difference between the original budget for the program and the currently estimated cost.

Response:

The modifications to Trilogy required as a consequence of the 9/11/01 attacks are articulated in response to Question 16, above.

18. You testified that the FBI had already implemented or begun to implement many of the recommendations contained in the May 2004 report of the National Academies on the Trilogy program. Please identify[:]

a. The specific recommendations that you have implemented;

Response:

Enterprise Architecture

Recommendation: The FBI's top leadership, including the Director, must make the creation and communication of a complete enterprise architecture a top priority. Status: The FBI Director briefed Congress regarding his commitment on 3/23/04.

Recommendation: The FBI should seek independent and regular review of its EA, as it develops, by an external panel of experts with experience in both operations and technology/architecture. Status: The FBI regularly seeks independent review of its EA by experts outside the FBI, including the Director's Science and Technology Advisory Board. For example, based on an October 2004 meeting with that Board, the FBI is expanding: (1) the Performance Reference Model, including validated outcomes; and (2) the development of an Interim Architecture, which will be used to assess current projects and to direct funding so as to ensure that the Bureau moves strategically toward a successful target architecture.

Recommendation: Given that the CT mission requires extensive information sharing, the FBI should seek input on and comment from other intelligence agencies regarding its enterprise architecture effort. Status: The FBI coordinates with the National Reconnaissance Office, National Geospatial-Intelligence Agency, Army Architecture Integration Cell, and others, and has requested review by the Intelligence Community System for Information-Sharing Implementation Board.

Recommendation: The FBI should build on the early efforts under way in the intelligence area in defining a sub-architecture for the intelligence process, rather than beginning with the VCF architecture. Status: The OI published its "Immediate/Near-Term Requirements" report on 6/30/04 and is developing its architecture in collaboration with the FBI's EA Program.

System Design

Recommendation: The FBI should plan to rework the next version of the VCF to include a workflow engine as a high priority. Status: This plan has been

completed and both VCF and any successor software will include a robust workflow management capability.

Recommendation: The FBI should adopt a risk management approach to security so that it can understand the operational penalties it pays for risk avoidance. Status: An IT Continuity of Operations Plan was initiated in January 2004.

Recommendation: The FBI should encourage creative experimentation with exploitation of IT in the field, such as the PDA experiment mentioned in section 2.2.4 of the report. Status: Research and Development with respect to the Blackberry Wireless has been completed, and the RAND Corporation is assisting with analysis of this effort.

Program and Contract Management

Recommendation: Because testing is such a critical dimension of system development and deployment, the FBI must allow adequate time for testing before any IT application (including VCF) is deployed, even if the dates of initial operational capability are delayed. Status: This has been approved under the Lifecycle Management Directive (LCMD) and transition for existing projects has been initiated.

Recommendation: Evolution is an essential component of any large system's life cycle. Future development contracts for user applications should be premised on the use of small-scale prototypes that can be built rapidly and tested with user feedback before committing to large-scale development. Status: The FBI concurs and has revised the VCF development consistent with this recommendation.

Recommendation: For IT applications beyond VCF, the FBI should exploit proven methodologies of contracting and contract management, including the use of detailed functional specifications, specific milestones, frequent contract reviews, and earned-value metrics. Status: The FBI's LCMD, which governs how IT projects are managed from "cradle to grave," is consistent with industry and other government agency best practices. All IT projects and programs will be required to pass through rigorous project and executive level control "gate" reviews for each state, from inception through disposal. The FBI is in the process of establishing an IT metrics program that identifies and measures IT performance according to industry standards, government regulations, and earned-value management system principles.

Recommendation: The FBI's contracting strategy should be tied to features of its EA; e.g., it should identify opportunities for multiple, smaller contracts with

well-defined deliverables and major progress checkpoints. This strategy should also highlight areas in which the FBI requires in-house or trusted technical expertise to define and manage key concepts that govern contracts and relationships between contractors. Status: This recommendation is implemented in the LCMD. Acquisition reform efforts will include consolidation of numerous existing contracts to leverage economies of scale and avoid duplication of effort. Strategies will be tied to EA, as appropriate.

Human Resources

Recommendation: Because of their importance to the short- and long-term success of the FBI's IT modernization efforts, the FBI must permanently fill the positions of Chief Information Officer (CIO) and Chief Enterprise Architect, and the committee concurs with the Director's judgment that filling these positions with appropriately qualified individuals should have the highest priority. Status: The position of CIO was filled in May 2004, and the positions of Chief Technology Officer (CTO) and Program Management Executive (PME) were filled in August 2004.

Recommendation: The FBI should develop an improved system for internally reviewing the state of progress in key IT programs and for communicating relevant findings to key stakeholders, thus preempting the perceived need for and distraction of constant external investigations. Status: The LCMD implements such a system.

b. The specific recommendations that you plan to implement, and when you plan to implement them;

Response:

Enterprise Architecture

Recommendation: The FBI should give high priority to reducing the management complexity of its IT systems, even at the expense of increased costs for hardware that may appear duplicative or redundant. Status: The LCMD establishes a structure by which new and existing IT proposals and systems will be evaluated to ensure they are being managed appropriately. Reducing management complexity is a priority in the development of the FBI's "To Be" or "target" architecture, scheduled for the late spring or summer of 2005.

Recommendation: The FBI should make heavy use of scenario-based analysis in its development of an enterprise architecture. Status: Phase II of the EA development includes scenario-based analysis, which will be included in the target architecture scheduled for the late spring or summer of 2005.

System Design

Recommendation: The FBI should develop a process map for information sharing that clearly defines the current state and a desired end state for the information-sharing process so that the numerous information-sharing initiatives can be coordinated and properly monitored and managed. Status: The FBI defers to DOJ, who is taking the lead on this recommendation.

Recommendation: The FBI should develop a future release plan for VCF that specifies what capabilities will be added to it, in what order, and in what time frame. Status: The FBI is employing a two-track plan designed to move us forward. Track One, also known as Initial Operating Capability (IOC), will test the Virtual Case File (VCF) prototype that has already been developed. Beginning in mid-January 2005 and for the following three months, personnel in the New Orleans field office, the Baton Rouge Resident Agency, and the Criminal Investigative Division's Drug Unit at FBI Headquarters will use the prototype VCF as their document routing system. This will assist the FBI in determining at least three things: 1) how easy the graphic interface is to use and how the electronic workflow process works from a business perspective; 2) what impact the prototype system has on the performance of the new Trilogy network; and 3) how training can be improved so that we can deliver the most helpful and user-friendly training possible Bureau-wide. Armed with these lessons and the new ACS interface, the FBI will move forward with Track Two - the development and delivery of a computer-based investigative case management system that will help the FBI meet its responsibilities to our country more efficiently. As part of the Track Two activities, the FBI has asked a new contractor to examine the latest version of the VCF as well as available off-the-shelf software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. In many ways, the pace of technological innovation has overtaken the original vision for VCF, and there are now existing products to suit the FBI's purposes that did not exist when Trilogy was initiated. The FBI has also asked a different contractor to review and verify users' requirements, because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing.

Human Resources

Recommendation: For Trilogy and subsequent IT projects to have access to the human talent they need to succeed, the FBI must dramatically grow its own internal expertise in IT and IT contract management as quickly as possible. Status: 25 IT managers have taken the EA Program Management Program review course, and 20 are currently enrolled in the program. A training curriculum for all IT employees is scheduled for implementation by the fall of 2005.

Recommendation: The FBI should seek relief from excessively tight constraints on reprogramming allocated funds, or at least seek to streamline the approval process. Status: The FBI hopes to accomplish this during FY 2005.

c. The specific recommendations that you do not plan to implement, and why you do not plan to implement them.

Response:

System Design

Recommendation: The FBI should refrain from initiating, developing, or deploying any IT application other than VCF until a complete EA is in place. Status: FY 2004 efforts include development of the "As Is" baseline and the EA Board. FY 2005 efforts will include initiation of the "To Be" architecture. Applications will include EA compliance and review as appropriate.

Recommendation: The FBI should immediately develop plans that address recovery of data and functionality in the event that essential technology services are subject to denial-of-service attacks (e.g., from viruses and pervasively replicated software bugs). Status: Some plans have been developed with respect to classified, mission-critical systems to provide system redundancy and fail-over capabilities. Broader, system-wide plans would require additional funding.

19. The National Academies report concluded that the Virtual Case File is not now and is unlikely to be an adequate tool for counterterrorism analysis, and that the FBI needs to start "more or less from scratch" to develop the operational requirements for its intelligence functions. Do you agree with the National Academies' assessment?

Response:

Following the 5/20/04 National Academies' report, the Committee on the FBI's Trilogy Information Technology Modernization Program issued a letter to Director Mueller, dated 6/7/04, highlighting the FBI's progress in addressing the report's findings. This letter acknowledged that VCF was designed primarily to enhance workflow automation, serving as the vehicle for various data feeds into analytical applications. One such application is the Investigative Data Warehouse (IDW) project, which encompasses CT activities as well as the deployment of criminal investigative capabilities. These capabilities will be extended Bureau-wide and to joint activities (including the JTTFs). IDW is a concept describing the preparation and organization of a variety of databases so they can be searched in a coordinated fashion along with other databases. This coordinated searching across several databases is known as advanced data analysis. IDW provides FBI investigators and analysts, particularly those

investigating terrorism and criminal conspiracies, with a new capability to easily and rapidly search and share information across all FBI investigative files, including text, photographs, video, and audio materials. It appears from the 6/7/04 letter that the Committee's understanding of the purpose and scope of VCF was assisted by a meeting at which FBI CIO Azmi explained this technology in more detail, including its role as one of the data feeds into IDW. Based on this preliminary information, the Committee indicated that "IDW appears to provide some of the key capabilities necessary for intelligence use."

20. Is it true that the FBI still does not have in place an automated system that will allow the FBI to share top secret and sensitive compartmentalized information internally and throughout the intelligence community or an automated system to allow FBI employees to readily access and share information throughout the FBI? Please explain your answer.

Response:

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

21. The OIG's December 2003 Report on the FBI's efforts to improve the sharing of intelligence and other information reinforced the need for the Virtual Case File and the problems with the Automated Case Support (ACS) system: "Under ACS, all documents, including ECs, require handwritten signatures; therefore, all documents are physically passed from person to person as they move through the review chain." Given the continuing delays in implementing VCF, are the procedures and paper-intensive approach of ACS still being used? Is there any plan in place to make the eventual transition to VCF easier? Are files, new and archived, being scanned and maintained on-line?

Response:

The current ACS file system utilized within the FBI does present limitations. ACS works adequately as a retrieval device to aid in the analysis and evaluation of information for investigative purposes. The system does not, however, support the sharing of important unclassified and classified materials with outside agencies. When ACS was developed, FBI investigations were primarily criminal in nature. Consequently, most investigations were not classified and those that were classified were classified at the secret level. ACS was developed to run on the FBI's internal network, which has been certified and accredited for secret-level information only and, therefore, cannot be used to transmit top secret or sensitive compartmented information. To rectify these shortcomings, the FBI initiated several methods of information sharing that afford the ability to electronically share and analyze both classified and unclassified information.

The FBI is increasing desktop access to the Internet by those with a need to share sensitive but unclassified information with law enforcement and IC partners. This

capability would also facilitate access to both the LEO and RISS networks. LEO is a national interactive computer communications system and information service; an intranet system exclusively for the law enforcement community. The RISS program is composed of six regional centers that share intelligence and coordinate efforts against terrorist and criminal networks operating in many locations across jurisdictional lines.

VCF was originally envisioned as a case management tool to replace the ACS system. In many ways, though, the pace of technological innovation has overtaken the original vision for VCF. Because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing, the FBI has asked Aerospace Corporation, a not-for-profit federally funded contractor, to review and verify FBI users' requirements. It is likely that VCF or its successor software will be deployed in phases, which will ease the transition for FBI employees.

22. If VCF is the system needed for the FBI to greatly improve the FBI's ability to share intelligence and other information, and if the current system was the critical weakness in the FBI's intelligence analysis and dissemination, what, if any, "stop gap" measures are currently in place to close the holes caused by the faulty and antiquated system the FBI is still working under?

Response:

The FBI is working on several IT improvements outside of Trilogy, including IDW, which permits sophisticated analysis of information from multiple data sources. The FBI has also changed its approach to IT to facilitate centralized management and to permit better coordination. The FBI now has a full-time CIO, who is responsible for the FBI's overall IT efforts, including: 1) developing an IT strategic plan and operating budget; 2) developing and maintaining the FBI's technology assets; and 3) providing technical direction for the re-engineering of FBI business processes. The CIO is in the process of formulating a strategic IT plan which takes into account the needs of the Intelligence Program, outside customers, and field and FBIHQ division needs. The FBI's Chief Technology Officer is responsible for guiding the IT research and development functions of the FBI. An EA Board, made up of 14 representatives from eight FBI divisions, meets regularly to review technical proposals for new FBI IT systems.

Translators

23. It has been nearly 3 years since Congress directed the Attorney General to prepare a comprehensive report on the FBI's translator program. I authored that reporting requirement – and it was a requirement, not a request. It was included in the USA

PATRIOT Act so that Congress could better assess the needs of the FBI for specific translation services, and make sure that those needs were met. The Foreign Translation Program is vital to our understanding of virtually every piece of intelligence information from the Middle East.

a. When will the report issue?

Response:

Section 205(c) of the Act required the Attorney General to provide a report to Congress on the employment of translators by the FBI and other components of the Department, but the Act did not specify the form or a timeline for submission of this information. The report called for by section 205(c) was transmitted to Congress on 12/22/04.

b. What are the current needs of the FBI for specific translation services? Is the FBI where it wants to be, right now, today, as of this moment?

Response:

Since the beginning of FY 2001, FBI audio and text translation requirements have increased by 51%. In several Middle Eastern languages, such as Arabic, collection has increased by more than 100%. Because of this increased demand, and despite an addition of several hundred translators during this period, unaddressed work remains in certain languages. Simply put, the growth in demand for FBI translation services has outpaced the increased translator supply.

The President's FY 2006 budget includes a $27 million enhancement to the FBI's language analysis program, supporting an additional 274 language analyst positions above the FY 2005 funded staffing level of 490 language analyst positions. This funding would greatly enhance the FBI's capacity to address intelligence collected in foreign languages in support of critical counterterrorism and counterintelligence investigations, to provide the National Virtual Translation Center with a permanent staff of linguists, and to address an expected FY 2006 deficit in the FBI's contract linguist program.

c. Are there any legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis? Have such options been explored? If not, why not.

Response:

The scarcity of qualified translators available to federal agencies, particularly among Middle Eastern and Asian languages, has been documented through

several studies (these studies include the 1/31/02 GAO report referenced above and a 2001 report by the National Commission on Terrorism entitled, "Countering the Changing Threat of International Terrorism"). Since most agencies' demands for translator resources exceed the supply, the concept of sharing translators is not practical, because each agency's natural tendency is to preserve limited resources for its own use. Such sharing is further impeded by non-uniform proficiency testing and clearance requirements.

Intermediate and long-range benefits of pooling federal translator resources are possible, but only if each federal agency is equally committed to the aggressive recruitment of translators and/or to the internal development of translator resources through language training. Otherwise, scarcity issues will continue to pose barriers to translator sharing.

There would likely be immediate, though limited, benefits from the pooling of IC and federal law enforcement translator resources in languages where demand is diminishing or shifting across agencies or where needs are sporadic. This is especially true when the lending agency has higher vetting and clearance standards than the receiving agency. For example, the FBI's current excess supply of Spanish CL resources could be immediately absorbed by DEA, Customs, or ATF because of the rigorous vetting and clearance requirements of the FBI. However, it would often be difficult for the FBI to absorb the resources of those agencies because most DEA, Customs, and ATF translators are cleared only for access to law enforcement sensitive information and not to national security information.

At the state and local law enforcement level, translation services are typically provided by police officers whose language proficiencies are uncertified or by CLs. While the FBI reviews any opportunities for resource sharing carefully, in most cases the law enforcement officer or translator does not possess the requisite security clearance to provide services to the FBI. For example, when the FBI's Chief of Language Services recently met with the Deputy Commissioner of the New York Police Department (NYPD) regarding the feasibility of such resource sharing, the NYPD indicated that they did not want their officers to undergo polygraph examinations, thus precluding them from receiving Top Secret clearances.

24. How is the monitoring of an unprecedented 1,727 new FISA wiretaps impacting on critical FBI resources? How do these numbers "translate" to the Bureau's ability to obtain, understand, assess, analyze and, if necessary, act upon threat information obtained in a foreign language and from a foreign culture?

Response:

While the number of wiretaps pursuant to the Foreign Intelligence Surveillance Act (FISA) has increased dramatically, the number of linguists to monitor these intercepts has also grown, from 883 linguists in 2001 to over 1200 linguists today. The FBI is continuing to process thousands of applicants to further enhance capabilities in the most critical languages. Although in the past the FBI's collection capabilities have outpaced its ability to process the materials acquired in several languages, successful hiring has eliminated the performance gaps in some languages and is steadily eroding the gaps between collection and review in other languages. The Language Services Translation Center at FBIHQ manages the FBI's translation resources, which are located throughout the country. The Center works closely with the FBI's operational program managers to prioritize the review of FISA materials, and will review previously untranslated material whenever the investigative value of the material becomes apparent.

25. When can we expect implementation of a statistical reporting system that will be able to track the status of translations so that the FBI can know what items are not being timely translated and provide insight as to why?

Response:

While the FBI has statistical reporting systems and other automated mechanisms in place to ensure the efficient use of translation resources, these systems are antiquated and mostly exist in a decentralized environment. To improve capabilities in this vital area, a Bureau-wide statistical reporting system known as Workflow Manager (WFM) has been developed for FISA electronic surveillance collections. WFM will measure review frequencies and production rates for trend analysis and command and control purposes. WFM is undergoing a test and evaluation process and is expected to become fully operational by the end of CY 2004.

26. Will data from translated material obtained through FISA wiretaps be included in the Virtual Case File system? If not, why not? How do agents and analysts currently do searches of FISA wiretap data to try to "connect the dots?"

Response:

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

27. Did the resources that the FBI requested DOJ to include in its 2005 budget request to fill performance gaps in the FBI's translator program differ in any way from the resources that DOJ ultimately sought in its 2005 budget request? If so, in what way? What other resources will assist the FBI in filling performance gaps.

Response:

Executive Branch agencies are not permitted to release pre-decisional data regarding budget requests. The President's FY 2005 budget requests an increase of 86 positions and $12.838 million for the FBI's Language Program.

28. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

Response:

There was no reclassification of any information at any time with respect to matters regarding Ms. Edmonds. Some information regarding this matter has always been classified. Other information was classified as of October 18, 2002, when the Attorney General asserted the state secrets privilege and DOJ moved to dismiss Ms. Edmonds' employment case. No further original classification occurred after October 18, 2002, and there was never any reclassification. We could provide a classified briefing for staffers who possess the necessary clearances.

Arrest Statistics

29. The GAO issued a March 2004 Report on Federal Law Enforcement on Use of Investigation and Arrest Statistics that appears to validate double or triple-counted investigation and arrest data to measure individual work load and performance. I think there is a need to distinguish among law enforcement agencies by valid statistics that can measure when an agency is actually working or simply piggy-backing on a multi-jurisdiction investigation to which they added little by way of resources or manpower. Congress often relies on the same data in determining FBI productivity and resource allocation. As GAO points out, if law enforcement agencies were to distinguish between unilateral and joint arrests and investigations within their databases, this distinction could help guide Congress when making budget decisions about these agencies. The agencies could modify those databases to reflect even more refined data. GAO also suggested that a

federal repository of joint investigations and arrests conducted by federal law enforcement is a good starting point.

a. Do you support the need for such a repository?

Response:

In light of the inherent complexities in the creation and maintenance of a centralized repository, we would need to determine whether the intended benefits would justify the added burdens and costs associated with the activity. For example, a single repository would require the integration of all federal agency information systems to efficiently report arrest-related data. Because numerous federal agencies (including numerous Inspectors General) have federal law enforcement authority, the creation of a single, integrated repository would be labor intensive. In addition to the need to assimilate potentially incompatible data, software, and hardware, such an effort would need to accommodate the fact that some information systems, including the FBI's, permit limited access for security reasons, so that integration with non-secure systems may not be supportable. Any process other than an automated integration would add manual reporting responsibilities, burdening personnel already overburdened with administrative responsibilities. Creation of a "federal repository of joint investigations and arrests" would also require the development of definitions that do not currently exist. For example, if the FBI conducts a multi-year, complex investigation and the U.S. Marshals Service assists only by effecting the arrests, would this constitute a "joint investigation"? If other organizations were not afforded appropriate "credit," would they be as willing to assist? If these organizations do receive a "joint investigation" credit, does this fairly represent the organizations' roles? Which organization would maintain and support the repository?

It is also critical to the FBI that the creation of a single repository not jeopardize interagency cooperation and coordination. As discussed below, there is a risk that changes to data reporting may appear to diminish the benefits participating agencies currently derive from assisting one another. The FBI would not perceive as advantageous anything that may jeopardize the growing inter-agency cooperation we have worked so hard to achieve.

b. What are the pros and cons of establishing such a repository?

Response:

A single repository would make it easier for GAO to track contributions to the federal government's law enforcement effort. The greatest disadvantages in establishing such a repository are the resources required to gather and report

information and the possible damage such reporting would inflict on critical joint working relationships.

Over the years, the FBI has forged partnerships with many state, local, and federal agencies in an effort to: (1) improve interagency cooperation and coordination; (2) maximize the development of intelligence in furtherance of inter-agency interests; (3) improve the effectiveness of operations; (4) take advantage of inter-agency talents, experience, and abilities; and (5) augment personnel resources to ensure mission accomplishment even when resources are limited.

If distinctions between unilateral and joint investigations are made, it will be important to ensure that these distinctions do not harm inter-agency cooperation. Joint investigations are often more successful when all parties share equally in accomplishments. This is particularly important in long-term, complex investigations in which smaller agencies offer the assistance of their limited personnel with the understanding that they will share equally in the investigative results and accomplishments even though the resources they commit are not as great as those contributed by larger organizations.

The FBI has always worked to afford appropriate credit to all participating organizations, regardless of the level of resource commitment. Sometimes the commitments of other organizations, while minor compared to those of the FBI, are particularly significant because they are based on that organization's expertise in a specialized area or unique ability to make a critical contribution, or are relatively more burdensome to that organization due to its very limited resources. Attempts to rate or categorize the relative contributions of various organizations is, however, quite difficult. If the FBI allocates five Agents to a highly complex white collar crime investigation, while the IRS commits one Agent, who would claim the "unilateral" indictment, arrest, and conviction accomplishments, and who would claim the "piggy-back" accomplishments? If the result of this investigation is the arrest of a prominent CEO of a major corporation and there is only one reportable accomplishment, how is credit assessed? Will organizations seek the credit most likely to be valued during congressional allocations of resources? If sufficient value is not attached, will the level of cooperation and coordination presently enjoyed be significantly impaired as agencies seek the credit most beneficial to their own interests in the congressional budget process?

c. Do you agree that the FBI should distinguish between unilateral and joint arrests and investigations? If not, why not?

Response:

The FBI believes it is important to distinguish between single, or "unilateral," agency arrests and multi-agency, or "piggy back," arrests, and that it is important

to apply uniform standards in reporting these accomplishments, provided this can be done without harming the joint working relationships that are often critical to investigative success, as indicated above.

Arrests are but one statistical accomplishment measured by the FBI. Generally, productivity in criminal matters is measured more by the numbers of high quality indictments and convictions because they are more indicative of the quality of investigative results and support for the affiliated U.S. Attorney's Office than arrest statistics alone. There are exceptions to this general guideline, such as when the arrest is the result of: an incident in which an Agent took direct action to save lives or property; or a fugitive investigation conducted in support of state, local, or international law enforcement authorities and the fugitive is believed to have been involved in serious violent crimes.

As noted in the GAO Report, the FBI credits each arrest only once, though an Agent who participates in an arrest can be credited with an "assist." If the arrest occurs in the context of an inter-agency investigation, this is reported in the FBI's Integrated Statistical Reporting and Analysis Application database. Although it is the FBI's understanding that, in multi-agency operations resulting in arrest, each participating agency claims an "arrest," the FBI is not aware whether other agencies report the multi-agency nature of the operation or whether they distinguish between arrests and assists.

First Responders

30. The Associated Press reported on May 26 that police in Vermont and New York will be able to check suspects instantly against the U.S. Government's terrorist watch lists under a "first-of-its-kind, FBI-coordinated program."

a. What is the name of the database system being used for this program?

Response:

The Upstate New York Regional Intelligence Center (UNYRIC) has an established Memorandum of Understanding (MOU) with CT Watch pursuant to which they submit a name check request for subjects who are stopped in circumstances consistent with possible terrorism activity. Under this agreement, CT Watch checks submitted names against the FBI's ACS system, the TIPOFF database, the FBI Watchlist, and the DHS Interagency Border Inspection System (IBIS) for possible terrorism watchlisting. The agreement provides for response within 20 minutes for "immediate" requests and within a reasonable amount of time for "routine" requests. The CT Watch has been performing these checks for UNYRIC since 2003 and sends facsimiles to requesters indicating search results.

The UNYRIC has always serviced the State of New York and recently entered into an agreement to provide these same services to the State of Vermont.

With the creation of the Terrorist Screening Center (TSC), the watchlist subjects in these databases are now uploaded into both ACS and DOJ's Violent Gang and Terrorist Organization File (VGTOF). The UNYRIC now receives hits from all of these databases by directly querying NCIC/VGTOF, and continues to send facsimile requests directly to CT Watch for subjects who are stopped in circumstances consistent with possible terrorism activity but on whom there is no NCIC/VGTOF hit. When these facsimile requests are received, they are checked against ACS (which now includes TIPOFF, IBIS, and VGTOF records) for any references to FBI-related matters.

b. When was it first available for implementation?

Response:

ACS has been used in UNYRIC requests since 2003, but the capability to search the uploaded TIPOFF, IBIS, and VGTOF records through ACS became available after the TSC began operations on 12/1/03.

c. What 12 databases will the Vermont police be able to check?

Response:

The database searched when the UNYRIC faxes a request to the FBI's CT Watch is ACS, which includes the TIPOFF, IBIS, and VGTOF databases.

d. Are the Vermont police being provided direct access to the databases or are they being provided a number to call at the FBI? Please provide more information on the "direct line" being provided to Vermont police to report suspicious activities to Federal law enforcement. Is the "direct line" a two-way line -- that is, will Federal law enforcement have a direct line to Vermont police about suspicious activities in Vermont?

Response:

The only direct access the Vermont Police have is through running routine NCIC/VGTOF queries (all U.S. law enforcement officials have the same capability). The Vermont Police send database check requests to the UNYRIC, which forwards the requests to CT Watch. There is no direct contact between the Vermont State Police and CT Watch (unless the State Police receive a VGTOF hit and go through the established process with the TSC). The UNYRIC may contact CT Watch through a direct telephone number to advise that a fax inquiry is being sent or to confirm that a fax was received. If the inquiry results in a hit, the

UNYRIC is notified and CT Watch puts an FBI Agent in touch with the UNYRIC directly.

The UNYRIC-CT Watch MOU provides a process for name check requests only, and it is not a mechanism for reporting "suspicious activity." The UNYRIC has a system in place by which suspicious activity deemed to be related to terrorism is reported directly to the appropriate FBI JTTF for immediate action. While the UNYRIC does not routinely report these matters to CT Watch, CT Watch notifies the affected JTTFs when this occurs.

e. What safeguards and/or technology protocols are in place to protect data security and privacy and to ensure that searches are pertinent to individualized investigations?

Response:

There is no transfer to the UNYRIC of information containing the specifics of FBI cases or TIPOFF records. The UNYRIC is simply made aware of FBI investigative interest and provided with an FBI case Agent or Field Division point of contact for further coordination. The CT Watch name check request form requests the justification for the name search, and this justification is reviewed by CT Watch personnel. If the justification does not relate to terrorist activities, the UNYRIC will be contacted to determine whether additional justification exits.

Ricin

31. Following the February 2004 ricin scare that shut down some congressional offices for as much as four business days, some of us learned for the first time there had been an earlier ricin attack directed at the White House. *USA Today* and other newspapers reported that ricin was first detected and investigated by the Secret Service on November 7, 2003, at an off-site mail processing center for the White House, although the FBI, the White House, and other agencies were not notified until November 12.

a. Is it correct that the FBI was not notified until November 12?

Response:

Yes. The FBI was notified by the Secret Service at approximately 10:30 p.m. on 11/12/03.

b. If the FBI learned about the attack in November, why was no information provided to the Congress or to other relevant high-priority targets of al Qaeda?

Response:

The texts of the two letters containing ricin, one of which was sent to the Secretary of Transportation and the other to the President, indicated that the ricin attacks were intended to cause the Department of Transportation (DOT) to make changes in the implementation of DOT trucking regulations. These threats were not related to al Qaeda or to international terrorism, and did not convey a threat to Congress or other high-priority al Qaeda targets.

c. Did the FBI ever notify State and local law enforcement officers? When and through what mechanism?

Response:

State and local law enforcement officers were notified on 11/13/03 through the National Joint Terrorism Task Force (NJTTF) and the JTTFs located in Washington, D.C., and Columbia, South Carolina.

d. Have there been any changes or policies implemented at the FBI based on the federal government's law enforcement response to the ricin attacks? If so, please describe in detail.

Response:

Yes. The FBI Laboratory and the Edgewood Chemical and Biological Center have begun efforts to develop more sensitive and dependable ricin detection methods. The FBI Laboratory has also begun closer collaboration with the Secret Service Laboratory in order to facilitate improved communication in these cases.

USA PATRIOT Act/FISA

32. You testified that many of the FBI's counter-terrorism successes are the direct result of PATRIOT Act provisions. Please provide more specific information on how particular PATRIOT Act provisions have helped in particular counter-terrorism investigations.

Response:

On 7/15/04, the Attorney General released "Reports from the Field: The USA PATRIOT Act at Work," which contains unclassified examples of cases in which the USA PATRIOT Act has been instrumental in counterterrorism investigations.

33. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state

specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response:

Prior to the changes effected by the USA PATRIOT Act, 18 U.S.C. 2517 was interpreted as authorizing the sharing of intercepted wire, oral, and electronic communications solely for criminal law enforcement purposes in the absence of a court order. Sharing intercepted information for foreign intelligence purposes required a court order, but the statutory language was unclear as to who would sign the order. The changes to the USA PATRIOT Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the Agents working intelligence cases.

34. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response:

Prior to the USA PATRIOT Act, there were procedures for sharing information between intelligence investigators and criminal Agents and prosecutors, but they were burdensome and usually resulted in less than complete information sharing. For example, the FISA statute was understood to require that, in order to secure a FISA Court order, the "primary purpose" of the activity had to be the acquisition of intelligence. Because of this interpretation, DOJ and the FISA Court placed procedural prerequisites on the sharing of intelligence with criminal investigators and prosecutors. Additional information is provided below in response to Question 35.

35. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002? How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

Response:

A distinction between the criminal investigation and intelligence functions existed before 1995, but the relationship between criminal and intelligence investigators became more distant as the"wall" developed and became more entrenched. In the years before FISA, and, indeed, in the early years of FISA, the relationship between criminal and intelligence investigators was closer than it was in 1995. In the 1980s, for example, criminal agents and intelligence agents were relatively free to talk to each other just as they had pre-FISA. Perhaps more significantly, prosecutors were free to give advice to both criminal and intelligence investigators because criminal process is always one option for the disruption of activities potentially harmful to the national security. By 1995, however, the wall precluded the sharing of all classified information – not just that which derived from FISA. Within a year thereafter, prosecutors were barred altogether from giving advice, and could only receive information about the progress of an intelligence case, unable to comment or make suggestions of any kind. Similarly, the intelligence agent and the criminal agent working related cases were by this time barred from discussing the intelligence aspects of the case, although criminal agents could disclose information to intelligence agents.

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing?

Response:

According to those who were directly involved in the case to which this memo refers, DOJ was trying to ensure that there were no artificial barriers to the flow of information. For those who were not involved in the specific case covered by the memo, the memo served to confirm that walls were necessary and that criminal investigators and prosecutors should not have access to classified information – even if that information was not obtained through FISA.

Inspector General Audit Report on FBI Information-Sharing

36. Please provide me a copy of the information-sharing process map recommended by the OIG in its Audit Report dated December 2003. If not yet completed, when do you expect the map to be completed and will you ensure that I receive a copy promptly?

Response:

The FBI's 12/5/03 Information Sharing Strategy was provided to the OIG pursuant to its recommendation that the FBI develop an FBI-wide enterprise architecture and process map. Because that report is **For Official Use Only**, and

therefore not appropriate for public dissemination, it is provided as an attachment to the Classified responses.

37. The Inspector General recommended in the December 2003 Report that certain domestic terrorism cases involving "lower-threat activities by social protestors or crimes committed by environmental, animal rights and other domestic radical groups or individuals (unless explosives or weapons of mass destruction are involved)" should be transferred to the responsibility of the Criminal Division as opposed to the Counterterrorism Division. The FBI rejected this recommendation, believing that the transfer would "dilute the intelligence base" directed to other international and domestic terrorism matters.

a. Has the investigation of these types of social protestors in fact led to useful leads in international terrorism cases involving, for example, al Qaeda?

Response:

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

b. Are criminal prosecutions of "lower-threat activities by social protestors" part of the "terrorism" arrest statistics reported by the FBI?

Response:

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

Domestic Intelligence Agency

38. The 9/11 Commission completed a critical report on the performance of the intelligence community with the statement: "A question remains: Who is in charge of intelligence?" The report described a "loose collection" of intelligence agencies that often operated independently of one another with little communication or cooperation, and concluded that the goal of central coordination has still not been realized. You told the 9-11 Commission it would be a "grave mistake" to have a separate domestic intelligence agency. Why? Another option would be a statutorily-created "domestic intelligence unit" within the FBI. What is your position on such a unit?

Response:

Creating a Separate Domestic Intelligence Agency

Creating a separate domestic intelligence agency would present numerous difficulties. While we cannot foresee every problem that would arise, we predict that the following challenges would impair the effectiveness of such an agency.

Operational Disruption

The logistics of transferring intelligence elements out of the FBI and establishing them within a new agency would disrupt the FBI's ongoing efforts to prevent terrorist attacks. The new agency would be required to develop the infrastructure the FBI has been building for the past 96 years. During this building process, the FBI's domestic intelligence efforts would be less organized and structured, and many of the FBI's leaders and decision-makers, who would otherwise be focusing on CT operations, would instead be devoting their time and attention on agency building. The result would be a lower level of preparedness and protection against terrorist attack.

In weighing this option, it is important to consider that al Qaeda has demonstrated its ability to adapt its plans based on an assessment of the United States' level of preparation, avoiding the strengths of U.S. defenses and exploiting vulnerabilities. In light of that intelligence, it is reasonable to assume that al Qaeda might attempt to exploit the disruption caused by the creation of this agency, particularly in the period before it is functioning fully.

Stove-piping

The creation of the new agency would likely recreate many of the obstacles to information sharing and operational coordination the FBI has worked hard to eliminate since the 9/11 attacks, building an operational wall between intelligence and law enforcement operations after the FBI succeeded in eliminating this impediment. The FBI and CIA have developed an effective process for coordinating the domestic and overseas dimensions of international terrorism investigations; movement of this responsibility to a new agency would complicate both the FBI's investigation of transnational terrorist threats and its inter-agency information sharing efforts. Finally, it would create the conditions for likely jurisdictional disputes, as the FBI and the new agency struggle to determine when a particular terrorist investigation is an "intelligence investigation" and when it is a "law enforcement investigation."

Diminished Ability to Cultivate Cooperators

There are two basic means by which an investigating Agent induces an individual to divulge information he or she is otherwise unwilling to provide. One is to promise the individual a benefit, such as money, if the information is provided. The other is to threaten to harm his interests, typically through arrest, prosecution, or deportation, if he refuses to do so. The FBI uses both approaches to develop and sustain its network of informants, sources, and cooperators.

An Agent in a separate intelligence agency without arrest powers would be handicapped in this process. While cooperation could be induced through the promise of benefits, the specter of imminent legal action would be unavailable. To gain cooperation in this manner, the new agency would instead have to obtain the assistance of a law enforcement officer, which would entail briefing the officer about the individual and waiting for that officer to receive authorization to initiate a criminal or immigration proceeding against the individual. This awkward and time-consuming process would complicate the recruitment process and render this new agency less effective in developing human intelligence.

This would be a serious handicap, especially given the general recognition that the lack of human intelligence relating to al Qaeda was the IC's most glaring operational weakness prior to the 9/11 attacks. The FBI has increased the number of its CT sources by 91% since 9/11/01, but it could not have done so without the full use of both recruitment methods.

Lack of Established Relationships with Law Enforcement

As the JTTFs have demonstrated, state and local police departments play critical roles in the war on terrorism. The FBI has seen in cases from Portland to Lackawanna that the 750,000 local police officers who know the communities around this country are often in the best position to learn about terrorist suspects in those communities. Without close collaboration with these officers, a federal agency coordinating an international terrorism investigation cannot expect to obtain the human intelligence it needs. While the FBI enjoys an excellent working relationship with state and local law enforcement that is borne of decades of collaboration, a new agency would be starting operations with no established relationship with the nation's 17,000 different police departments. That relationship could be developed over the years, but our nation's defenses against terrorism would be weakened in that interim.

Fragmented Accountability

Currently, the Attorney General and the FBI Director are jointly accountable to the President for both the law enforcement and intelligence components of CT and CI operations within the United States. Separating and assigning the intelligence component to a new agency will simply fragment accountability and make it more difficult to assign responsibility.

Cost

Proponents of the MI5 proposal have largely ignored the fiscal implications of creating a new agency. It would, in fact, be very expensive to build this new agency, the cost of which would not be covered by transferring the intelligence

funding that was previously allocated to the FBI for several reasons. First, the Bureau would still need a significant portion of those funds to develop and sustain the intelligence program needed to support its remaining areas of responsibility. Second, the new agency would require a substantial front-end investment, significantly greater than the cost of strengthening the FBI's intelligence capacity, to build the basic elements of its infrastructure, such as the facilities, information technology, and administrative operations necessary to support such an agency. The new agency would be competing for these resources with the existing members of the federal law enforcement and intelligence communities.

Conclusion

These considerations make it clear that creating a separate agency to collect intelligence in the United States would be a grave mistake. Splitting the law enforcement and intelligence functions would leave both the FBI and the new agency fighting the war on terrorism with one hand tied behind their backs. The distinct advantage gained by having intelligence and law enforcement together would be lost in more layers and greater stovepiping of information, even after completion of the difficult transition to the new agency, which terrorists may well see as an opportunity for attack. The FBI's strength has always been, and still is, in the collection of information. While there have been weaknesses in the integration, analysis, and dissemination of that information, the FBI has made great strides in addressing these weaknesses. The United States has a tremendous resource in the FBI. It would be both more efficient and more effective to improve that resource than to replace one of its primary functions with a new agency.

Statutory Creation of a "Domestic Intelligence Unit" in the FBI

The FBI supports the concept of an intelligence service within the FBI. This concept consists of two basic components: (1) creation of a new Directorate of Intelligence, and (2) more effective use of resources. These components can be addressed by applying the following principles.

First, any reform proposal must recognize that intelligence is fundamental to successful FBI operations. Intelligence functions are woven throughout the fabric of the FBI, and any changes to this integrated approach would be counter-productive. Intelligence capability is embedded in every aspect of the FBI workforce and organization - in the Agent and analyst populations, and in the Laboratory, Cyber, Investigative Technologies, and Training Divisions. Because of this integration, the FBI can analyze the devices and techniques of our adversaries, making information acquired from them available to our partners in the IC and in state and local law enforcement.

Second, the FBI must continue to integrate intelligence and law enforcement operations, employing both intelligence and criminal investigation tools as parts of an integrated CT strategy that affords the flexibility to move seamlessly from intelligence gathering to disruption at a moment's notice.

Third, analysis should be fully integrated into intelligence collection and other operations so that intelligence can drive the investigative mission.

Fourth, the FBI should have centralized management with distributed execution. Central management should support national collection efforts, information sharing, and dedicated strategic analysis that pulls intelligence from all FBI offices and across all programs, and ultimately drives planning and the allocation of resources.

And fifth, the FBI should limit stovepiping of intelligence collection and analysis, and encourage synergy in its operations and in collaboration with partners.

With these guiding principles in mind, the FBI supports the creation of a strong intelligence service within the FBI that leverages its formidable collection capabilities and fully integrates its efforts with its law enforcement and IC partners.

The first step toward this "service within a service" is to build upon the FBI's existing Office of Intelligence to create a Directorate of Intelligence with broad and clear authority over intelligence-related functions. The authority of the FBI's Executive Assistant Director for Intelligence (EAD-I), who now provides policy and oversight, would be extended to cover all intelligence-related budgeting and resources.

This structure would support each critical intelligence-related function, beginning with the critical function of management of the FBI's intelligence requirements process - the ongoing cycle of identifying intelligence gaps and directing collection to fill those gaps.

Management of Intelligence Requirements and Collection

The FBI currently has an Intelligence Requirements and Collection Unit that provides independent and centralized management of its intelligence requirements and collection functions. The efforts of this Unit would be strengthened by: (1) working with target experts to develop collection strategies to fill gaps in knowledge; (2) developing, implementing, and overseeing FBI standards for the validation of assets and sources; and (3) making intelligence from human sources available across program lines.

Information Sharing

The EAD-I is responsible for information-sharing policy, and the FBI expects demands in this area to increase. In particular, the FBI must participate fully in the Justice Intelligence Coordinating Council (JICC), DOJ's Law Enforcement Sharing Initiative, the Director of Central Intelligence (DCI) Advisory Group, and other entities.

The FBI's contingent at the Terrorist Threat Integration Center (TTIC) would be part of the FBI's Intelligence Directorate and would be fully incorporated into the FBI's information-sharing efforts.

Customer Support

To enhance the FBI's support of outside customers in state and local law enforcement, the Directorate would evaluate customer satisfaction, tailor the FBI's support to each major customer, and ensure that these partners are receiving the information they need from the FBI.

Strategic Analysis

To boost the FBI's strategic analysis efforts, the new Directorate would be responsible for the organization and implementation of strategic intelligence campaigns to support major cases, crisis response, and significant threats. The Directorate would work with operational counterparts to design, organize, implement, and manage an FBI intelligence system support structure.

The proposal also envisions promoting enterprise-wide strategic analysis through the development of analytic products that cross traditional programmatic lines and identify intelligence gaps to facilitate the development of collection and dissemination requirements. This analysis would help the FBI forecast future threats, and would drive the allocation of resources and the development of investigative and intelligence strategies in support of the FBI's mission. This is analogous to the DCI's National Intelligence Council (NIC), which ensures a full-time focus on strategic issues.

Intelligence Production and Use

To support intelligence production and use, the FBI would build upon existing units to improve its 24-hour intelligence production capability, FBI daily reports, and the FBI's Presidential Intelligence Assessments.

Field Operations

To support intelligence activities in the field, the FBI would integrate intelligence received from Legal Attachés into the FBI's overall intelligence capability. The Field Intelligence Groups (FIGs) would be thoroughly integrated into the larger IC. The FBI would also focus on the new regional intelligence centers, such as the recently announced CT Unit at the Upstate New York Regional Intelligence Center.

Human Talent

To support vital functions related to human talent, the FBI would create a new Intelligence Career Management group to manage the intelligence career track for Agents, intelligence analysts, linguists, and others, including the development of intelligence training across the FBI. An FBI Intelligence Officer certification program would be developed, and would include IC Officer Training. These efforts would enable the FBI to build on its efforts to create career paths for analysts and intelligence Agents.

Language Analysis

The FBI's linguists are responsible for more than straight translation. To be effective, they must be familiar with those involved and understand the context in which they are translating. This is fundamentally an analytical function and, accordingly, the FBI's language analysts should be fully integrated into the Intelligence Program as well as into operations. To support this integration, the Language Services Section and the National Virtual Translation Center would be moved to the Directorate of Intelligence.

Program Management and Support

Last, but important to the success of this proposal, would be the strengthening of program management support to the EAD-I and across the elements of the Intelligence Program. Emphasis would be placed on: ensuring that FBI Intelligence Program priorities are consistent with those of the DCI , DOJ, and other critical parties; developing the annual Future Threat Forecast; and providing security planning and guidance. Budgeting, evaluations to measure progress, communications and administrative functions, and support for the EAD-I's role as Chair of the JICC would also be emphasized.

Budgeting

Formalizing and strengthening centralized management of all intelligence-related resources would be among the key responsibilities of the new Directorate. The OI's initial effort has been the development of the Concept of Operations for Intelligence Budgeting, but it can and should move further. The President's Fiscal

Year 2005 Budget proposes restructuring the FBI's budget decision units from the current ten to four, one of which would be an Intelligence Decision Unit. Similar recommendations have been made by members of the legislative branch and the National Association of Public Administrators. This change would allow the FBI to more effectively and efficiently manage its resources based on national priorities and threat assessments, providing the flexibility needed to internally shift resources to higher priorities and to respond to rapidly developing national security threats. If this change is effected, the Intelligence Decision Unit would be comprised of operational elements, including the existing OI, the FBI's TTIC contingent, programmatic elements representing analysts across the FBI, and administrative elements, such as training, recruitment, information technology, and security. Creation of this Decision Unit would provide internal safeguards for intelligence resources by requiring Congressional notification if funds are reprogrammed, and would permit easier assessment of the level of resources supporting the FBI's intelligence program.

Indonesia

39. In August of 2002, two Americans and one Indonesian were murdered near the Freeport gold mine in Indonesia. Patsy Spier, the wife of one of the Americans killed, has done an extraordinary job of raising awareness of this crime, and has pressed the United States Government to determine who was responsible. The FBI has gone to Indonesia a number of times to investigate this crime, and until recently, has encountered resistance from the Indonesian Military (which is probably responsible for the crimes). Patsy Spier met with you earlier this year and you pledged to see the investigation through to its conclusion. Can you share the status of this case with me? I have worked to condition some military assistance for Indonesia on the government's cooperation with the FBI. Has there been cooperation? Can I have your personal assurance to see that justice is done in this case and that it does not fall through the cracks?

Response:

During the first 14 months of this investigation, cooperation by the Indonesian military (TNI) was assessed as "poor" by the FBI. Since the FBI team traveled to Indonesia in December of 2003, cooperation has dramatically improved, and is currently assessed by the FBI as "good." This is in large part because of the pressure applied by Congress and the Administration, both of which have directly engaged Indonesian officials.

The FBI independently developed sufficient evidence to obtain a 6/16/04 indictment in U.S. Federal Court. The subject charged with the 8/31/02 murders is Anthonius Wamang, a member of the military branch of the Free Papua Movement, commonly known as OPM. The FBI has devoted significant effort to determining if the TNI was responsible for or involved in this attack. To date, the

FBI's investigation indicates that the TNI was not responsible for these murders. You have our assurance that the FBI will continue to pursue this matter to ensure that justice is done.

Data Mining

40. Data mining is a potentially critical information technology tool for investigating terrorism and other criminal activity, but it also poses significant challenges for privacy, data accuracy and security, and civil liberties. Well over a year ago, I began writing letters to the Department about its data mining projects and related safeguards, but the Department has failed to answer the questions. For example, on January 10, 2003, I wrote the Department seeking information on private sector databases obtained for data mining or pattern-recognition activities. On March 22, 2004, I questioned the Department about the DOJ-funded MATRIX program, its privacy and security protections, as well as its use of data mining techniques like the "terrorism factor information query capability" to search billions of records -- many of which belong to individuals with no criminal history. I still have not received answers to these letters. Even more disappointing is that in many cases, my colleagues and I have had to rely on information released by press accounts, often addressing the same issues that the Department has failed to answer. It is inexcusable that the Department has failed to answer these letters. When can I expect answers?

Response:

DOJ responded to your letter of 1/10/03 by letter dated 6/8/04, and to your letter of 3/22/04 by letter dated 6/18/04.

41. It was recently reported that following the 9/11 attacks, the nation's largest airlines responded to a sweeping request from the FBI for as much as a year's worth of passenger records, including names, addresses, travel destinations and credit card numbers. The FBI's request was different from its typical requests to airlines, which usually concern passengers on single flights, or the travel patterns of individual passengers. At least one airline went so far as to set up extensive facilities for FBI agents in its headquarters. Reportedly, the FBI developed "a model of what these hijackers were doing" and then searched the passenger data for patterns, an activity which largely resembles a data-mining operation. But as an FBI official stated in the *New York Times*, "[t]here is no indication that the passenger data produced any significant evidence about the plot or the hijackers."

a. What privacy and security protections were employed in this search of individual airline data?

Response:

The purpose of this FBI project was to construct a time line reflecting the travel of the 19 9/11/01 hijackers leading up to the attacks. Subpoenas or official letters requesting records related to these hijackers were used as necessary, and some information was provided voluntarily by airlines (because the focus of the FBI's inquiry was on international flights, FBI investigators worked with both U.S. and non-U.S. airlines; non-U.S. airlines were less likely to require U.S. subpoenas). In some cases the FBI identified those sitting next to or in close proximity to one of the 19 hijackers to try to identify potential associates, but information concerning these passengers was not the focus of the initial request to the airlines.

The information obtained by the FBI was maintained in a secure area. When FBI personnel were not physically present, the information was maintained in a locked safe to which only FBI personnel had access.

b. What type of models or criteria were used to search the records?

Response:

Initially, available lists of passengers on Middle Eastern flights were collected and reviewed. This was done only to identify passengers who appeared on more than one flight with a hijacker. To expedite analysis, commonalities with the 9/11 hijackers were established, such as Middle Eastern males having dates of birth (when available) near those of the 9/11 hijackers. Seat assignments were also used as a guide because the hijackers mainly flew first class. No further review was conducted with respect to passengers who shared only one flight with a hijacker, since the project focused on identifying individuals who traveled more than once on the same flight as one of the 19 hijackers.

c. Was this data ever merged with any other government database?

Response:

The flight manifests were scanned into Intelplus and passenger names were entered into ACS. In addition, the Foreign Terrorist Tracking Task Force (FTTTF) was given a copy of the passenger/travel database.

d. Did these searches lead to any investigations, arrests or prosecutions, and if so, where these actions based solely on the search results, and what were the results of those efforts?

Response:

Out of a pool of over 6,000 passengers, the project identified 44 individuals believed to require further review, and several FBI Field Offices opened investigations on one or more of these individuals. However, as most of the travel records did not contain identifiers for these passengers, the Field Offices typically view these identifications as valuable only for name match purposes, with additional investigation being needed to match a subject with a passenger on a hijacker's flight. These investigations are ongoing. The names of these 44 individuals were forwarded to the CIA.

e. Does the Department still have possession of this airline passenger data, and if so, for what purposes is it being used and what are the plans for the data?

Response:

The passenger data is currently boxed, sealed, and ready to be inventoried as evidence. These boxes will be delivered to the FBI warehouse facility so that they will be available for possible use at the upcoming Moussaoui trial.

42. Recent reports indicated that "a key selling point" for the Department in awarding funds to Seisint, Inc. for the MATRIX program was the company's data-mining technique -- the "high terrorism factor" scoring system, which incorporated factors like age, gender, ethnicity, credit history and information about pilot and driver licenses. Reportedly, this scoring system identified 120,000 terrorism suspects and led to investigations and arrests. In addition to answering my March 22 questions about MATRIX, its terrorism scoring system and use by DOJ in investigations, please also answer the following:

a. Reports indicate that the scoring factor is no longer in use in the MATRIX program. Please confirm whether the scoring factor or any other data mining technique is currently a part of the MATRIX program. If so, please describe those techniques (*e.g.* whether identification, link-analysis, or pattern analysis), the success of use, and any privacy, accuracy or security protections. If not, please indicate whether there are any plans to include the scoring factor or any other data mining technique in future uses of the MATRIX program.

Response:

While the MATRIX program was not developed or managed by the FBI, those in DOJ who are knowledgeable regarding this program have advised as follows.

The Factual Analysis Criminal Threat Solution (FACTS) application used by MATRIX is not able to conduct pattern recognition or predictive analysis. Queries, which may be posed by law enforcement investigators or analysts, will

elicit only records matching the specific request. While a scoring factor called a "High Terrorism Factor" (HTF) was used for a limited time with respect to the 9/11/01 attacks, and proved successful in developing investigative leads in conjunction with the 9/11 investigation, this is the only investigation in which the HTF factor has been used and there are no plans to use it in MATRIX applications.

The HTF, or "terrorist quotient," was developed in the aftermath of the 9/11 attacks, when commonalities among the 19 hijackers were developed by Seisint's technicians, along with representatives from the FBI Miami Field Office, INS Miami Region, Secret Service Miami Office, Florida Department of Law Enforcement (FDLE) Miami Office, and U.S. Customs Miami Office. The HTF combined patterns and anomalies to identify individuals who shared characteristics and commonalities with these 19 hijackers. Once these individuals were identified, human investigative and analytical efforts were applied to determine whether any of them did, in fact, have any involvement in the 9/11 attacks or other terrorist activities. Without this human analytical intervention, application of the HTF would have had no investigative value.

The HTF capability was subsequently enhanced by combining commercially available data and state-contributed public information, resulting in an application called "Florida Crime Information Center - Plus" (FCIC+), so called because it was a single-query interface between the criminal history records maintained by the FCIC "plus" the Accurint public data maintained by Siesint, Inc. Access to the HTF tool within FCIC+ was "locked" by security software and strictly limited to four senior FDLE investigators/analysts, as well as a few Seisint technicians (whose access was to permit application development and testing).

The individuals identified through application of the HTF were not terrorist "suspects," but instead were individuals who had characteristics similar to the 19 hijackers. Only through further investigation of these individuals could any possible suspects be identified. Upon conclusion of this investigation, the investigative team disbanded and returned to their respective agencies, though the FDLE's representative remained on-site to work with Seisint technicians to develop an investigative tool that would combine and apply commercially available data, public information, and law enforcement data subject to limited dissemination (such as drivers' licenses and photos, vehicle registrations, criminal and corrections histories, and sexual offender data).

During this same time period, at least 15 states were involved in significant discussions on how better to share information and intelligence to prevent future terrorist attacks. Many of these states later became the originating participants in the MATRIX Pilot Project. The success of the FCIC+ application, including the HTF, was demonstrated to these states as an effective means of sharing data and

performing factual data analysis. The FCIC+ application was further enhanced, and evolved into the present FACTS application. After careful consideration by project participants, including consideration of security and privacy concerns, it was decided that the FACTS application, which was to be included in the MATRIX Pilot Project, would not contain the HTF functionality. This decision was made in the course of discussions as the project progressed and was not memorialized in the form of a memorandum or meeting minutes.

b. 120,000 is a very large number of suspected terrorists, and if accurate, would suggest a substantial threat. How many of the 120,000 suspects were subject to further investigation, arrest or prosecution, and what were the results of those efforts? Were any of the 120,000 successfully prosecuted for terrorist activity?

Response:

The list of 120,000 names was compiled and delivered to law enforcement before the MATRIX Pilot Project was initiated. As indicated in response to subpart a, above, Seisint created and provided a list of individuals (not "suspects") to an investigative team following 9/11/01. This team was not associated with the MATRIX project. Upon conclusion of the team's efforts, the members assigned to the team disbanded and returned to their respective agencies. Because investigations could have been conducted by any of the agencies participating on this team, it is unknown how many of these individuals were investigated.

c. Was there a process for determining whether any of the 120,000 individuals should be removed from the list or cleared of any association with terrorism activity, and if so, what was that process and how many individuals were cleared?

Response:

As indicated in response to subpart a, above, the purpose of compiling a list of individuals who shared commonalities with the 19 hijackers was as to determine whether any of these individuals were, in fact, associated with terrorism. The list was not considered or used as a list of "suspects."

d. Were any of the 120,000 individuals included in the terrorist watch list compiled by the Terrorist Screening Center, and if so, how many?

Response:

Mere inclusion on the list of 120,000 individuals, without the development of additional information through investigation, would be an inadequate basis for inclusion on the Terrorist Screen Center (TSC) watch list. Nominations for the inclusion of international terrorists are provided to the National Counterterrorism

Center (NCTC), which determines whether to forward the nomination request to the TSC. Records forwarded to the TSC by the NCTC are adjudicated by the TSC to determine whether they are appropriate for inclusion in the TSC database.

43. Recently, the Technology and Privacy Advisory Committee, which was appointed by Secretary Rumsfeld, issued a report on data mining. That report stated "[W]e believe that there is a critical need for Congress to exercise appropriate oversight, especially given the fact that many of these data mining programs may involve classified information which would prevent their being disclosed in full publicly. At a minimum, we believe that each agency's privacy officer and agency head should report jointly to appropriate congressional committees at least annually on the agency's compliance with applicable privacy laws; the number and nature of data mining systems within the agency, the purposes for which they are use[d], and whether they are likely to contain individually identifiable information about U.S. persons; the number and general scope of agency findings authorizing data mining." Do you agree with this statement? If not, please explain to what extent you disagree and your reasons.

Response:

This question refers to the March 2004 report of the Technology and Privacy Advisory Committee (TAPAC), entitled "Safeguarding Privacy in the Fight Against Terrorism."

While the FBI agrees that information on FBI privacy law compliance should be made available to Congress and the public, present reporting requirements ensure appropriate disclosure. DOJ's Management and Planning Staff (MPS) maintains DOJ's official Privacy Act inventory and manages the administrative processing of notices and rules, and the FBI periodically advises DOJ of the status of FBI compliance with privacy laws. Reporting requirements include biennial matching activity reports, reports on the establishment of new "systems of records," and reports with respect to the modification of a "system of records" when a new routine use or exemption is added or a system of records is otherwise altered. These reports are submitted to OMB and both houses of Congress. In addition, the E-Government Act of 2002 requires agencies to report annually to OMB on agency compliance with that Act.

The second and third recommendations (regarding reports on the number and nature of data mining systems within the agency and the purposes for which they are used) both concern data mining. The FBI is concerned that there is a lack of consensus regarding the definition of "data mining." The TAPAC report defines "data mining" as searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government. Under this definition, the second and third recommendations become nearly impossible to implement. If data mining is any search of an

electronic database, then "the number and nature of data mining systems," would include every system on a computer within the FBI, and encompass all searches of all databases. As a criminal investigative agency, the FBI conducts thousands of records searches a day, all of which are fully in compliance with the Privacy Act and other applicable privacy laws. Under these circumstances, providing a report on "the number and general scope of agency findings authorizing data mining" pursuant to this definition would be extremely burdensome, inhibiting the FBI's investigative functions in the absence of additional resources and staffing.[1] Even if such reporting could be accomplished, it appears that these reports may be so broad that they would not provide information helpful to Congress in exercising effective oversight.

In assessing the need for additional reports in this area, it is important to recognize that the development of any new system affording the FBI access to data in ways that were previously technologically unavailable requires a Privacy Impact Assessment (PIA) to ensure that the new system complies with all privacy laws. The FBI had established such a process well before the E-Government Act required it, and both that process and the subsequent PIA process assure compliance with applicable laws, regulations, and policies governing individual privacy and provide FBI officials with an assessment of a proposed system's impact on privacy. The PIA process includes a review of new or modified systems by FBI legal staff and the FBI Senior Privacy Official. If warranted, proposals are submitted to the FBI Privacy Council for review and comment. Through this process, both Privacy Act compliance and privacy policy issues are addressed. DOJ is currently developing standardized PIA procedures.

The following 26 questions from Senator Leahy request additional information with respect to questions posed following the 7/23/03 oversight hearing, to which the FBI has previously responded.

44. (Follow-up to Leahy 2) Have you completed the review of the manuscript submitted by SA Robert Wright for publication? If so, when, and has SA Wright been notified? Were portions of the manuscript determined to be "objectionable" and why?

Response:

As indicated in the FBI's earlier response, Mr. Wright submitted an amended "Fatal Betrayals" manuscript in February 2002, and this manuscript was provided

[1]The GAO Report entitled "Data Mining: Federal Efforts Cover a Wide Range of Uses," GAO-04-058, defines "data mining" as the application of database technology and techniques, such as statistical analysis and modeling, to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results. This definition, while narrower, is still not specific enough to provide the necessary guidance as to which systems should be reported.

to the FBI's Chicago and Milwaukee Divisions and to the U.S. Attorneys' Offices for the Northern District of Illinois and the Eastern District for Wisconsin for review. In May 2002, the FBI advised Mr. Wright that the manuscript contained information regarding open investigations, matters occurring before a federal grand jury, sensitive law enforcement techniques, intelligence, and information otherwise prohibited from release, and that the manuscript, as drafted, could not be published.

In June 2002, Mr. Wright appealed the prepublication review decision to the Director of the FBI; that appeal was denied in July 2002. A November 2002 appeal by Mr. Wright to the Associate Deputy Attorney General was denied on procedural grounds (appeal to that level is available only based on the inclusion of classified information in the submission, and the amended transcript did not include such information). In October 2003, Mr. Wright was advised that a recent re-review of the manuscript had resulted in the determination that Chapters 1-4 and pages 103-16 and 119-22 of Chapter 7 could be published, but that the remainder of the transcript remained unapproved for publication.

45. (Follow-up to Leahy 3B) Has FINCEN finished preparing rules regarding precious gems as required by the USA PATRIOT Act? What is the status of the rules? What is the reason for the delay in promulgating the rules?

Response:

FinCEN, which is part of the Department of the Treasury, is in the best position to provide an update on the status of this matter.

46. (Follow-up to Leahy 4) Based on your response, I understand that individuals who were not named recipients of the Phoenix EC could not query ACS using search terms and locate the document. Given that "two Agents on international terrorism squads in the New York Office" were "recipients," in that they were on the addressee line of the Phoenix EC, would they have been able to query ACS prior to September 11, 2001, using search terms and locate the EC? If so, how? Under the ACS system being used today, can all agents and analysts query ACS using search terms and locate any ECs containing that search term within the FBI? Will this capability be different under the Virtual Case File and if so, how?

Response:

The search capabilities of the ACS system were explained to this Committee by letter dated 6/14/02. This issue was again addressed in response to your Question 3 posed to Director Mueller following the 6/2/02 Committee hearing. That response was transmitted to the Committee by letter from Assistant Attorney General Moschella dated 7/22/03. In addition, we reiterate our request that

members of the Committee visit FBI Headquarters for an online demonstration of our current search capabilities.

The Trilogy program will eliminate the need for complex ACS searches, permitting the use of simpler and more intuitive search functions, similar to those used with Internet search engines.

47. (Follow-up to Leahy 6) Under 50 USC § 2655, the FBI and the Department of Energy are required to consult on regulations necessary to carry out the Counterintelligence Polygraph Program. By statute, those regulations shall include procedures for (1) identifying and addressing "false positive" results of polygraph examinations; and (2) ensuring that adverse personnel actions not be taken against an individual solely by reason of that individual's physiological reaction to a question in a polygraph examination, unless reasonable efforts are first made to independently determine through alternative means the veracity of that individual's response to that question. Have such regulations been drafted, promulgated or implemented?

Response:

The Department of Energy regulations are published at 10 C.F.R. Part 709.

48. (Follow-up to Leahy 6) You note two differences in the Grassley-Leahy FBI Reform Act and the FBI's current polygraph program. The first involves the class of persons subject to a polygraph; the second involves the need to administer random, five-year periodic and compelled polygraphs where appropriate. Can you propose specific language to address these differences, such that you could support this provision of the FBI Reform Act?

Response:

As the FBI indicated in response to questions following the Director's 7/23/03 hearing, the population subject to polygraph is comprised of those with access to sensitive FBI information, and these polygraphs are administered, pursuant to established criteria and procedures, on a periodic basis, on an aperiodic (random) basis, and when necessary to resolve particular security concerns. The FBI has designed its polygraph program to protect both FBI information and those who have access to it, using the polygraph as one tool among many to ensure the continued trustworthiness of those using and disseminating sensitive FBI information. The FBI would be pleased to work with DOJ and Congress to develop language that meets the needs of the FBI in fulfilling its intelligence and law enforcement missions.

49. (Follow-up to Leahy 7A) When did the FBI begin drafting the provision "currently under review" that "clearly prohibits an FBI agent from having any sexual relationship with a cooperating witness? Has the review process been completed and can I have a copy of the new policy? Would violations of this policy be deemed a "performance" issue or a "misconduct" issue?

Response:

The FBI policy prohibiting inappropriate relationships between Agents and Confidential Informants (CIs) extends to the handling of all FBI human sources. In August 2003, a provision was drafted to clearly prohibit an FBI Agent from having any sexual relationship with a cooperating witness (CW). This provision was approved for inclusion in existing policy in November 2003, and was subsequently published in the Manual of Investigative Operations and Guidelines, Part 1, Section 270-4(12)(a). This provision states: "While an Agent is permitted to socialize with a CW to the extent necessary and appropriate for operational reasons, the Agent is never permitted to engage in an intimate and/or sexual or unduly familiar social relationship with a CW." Violation of this policy would be handled as a "misconduct" issue.

50. (Follow-up to Leahy 7C) Did any FBI employee report any suspicions with respect to Agent Smith's relationship with Katrina Leung and, if so, how was such report handled?

Response:

No suspicions of a possible relationship between SA Smith and Ms. Leung were reported to the FBI's Office of Professional Responsibility, which is responsible for addressing allegations of employee criminality and misconduct.

51. (Follow-up to Leahy 10) How many full-time agents were assigned to civil rights investigations through the end of FY 2003 and how many have been assigned to date in FY 2004? Given that there were at least "the equivalent of" 74 fewer full-time agents in FY 2003 working civil rights than there were in FY 1999, what happened to open civil rights investigations that the 74 agents were working when reassigned? How many cases have been declined because no agents or analysts were available to work them?

Response:

In FY 2003, the equivalent of approximately 114 full-time Agents were assigned to civil rights investigations. Through the end of March 2004, the number of full-time Agents working civil rights matters rose to just over 120.

Although there has been a decrease in the number of full-time Agents working civil rights matters since a high of 190 in FY 1999, all civil rights investigations

continue to be investigated aggressively and thoroughly. If an Agent who is assigned to investigate civil rights matters is reassigned to another investigative program or otherwise leaves the FBI through resignation or retirement, the Agent's civil rights cases are reassigned to another Agent, who will be responsible for those cases until all investigative leads are exhausted. Every civil rights investigation is forwarded from the field to the Civil Rights Unit (CRU) for review with respect to completeness, among other things. In addition, the Criminal Section of DOJ's Civil Rights Division and the local United States Attorney's Office (USAO) receive copies of civil rights investigations, and either office can request additional investigation.

The CRU is aware of no instance in which the FBI declined to investigate a civil rights complaint due to the unavailability of civil rights personnel. Any civil rights complaint that appears on its face to be a violation of a federal civil rights statute is opened and investigated thoroughly.

52. (Follow-up to Leahy 11) Based on the summaries you provided, the FBI successfully concluded 41 civil rights cases in FY 2002 through the 3rd quarter of FY 2003 as the "lead investigative agency." Of those, approximately 20 appeared to fall under your definition of a "hate crime"; 15 were "color of law", 2 were "freedom of access," and 4 were "involuntary servitude and slavery" cases. I appreciate that these are complex, difficult cases, but these low numbers concern me, particularly because the number of agents working these time-intensive investigations is rapidly declining. Given the importance of these cases, which State and local authorities often cannot handle or have requested Federal assistance in handling, what recommendations do you have to ensure that the FBI continues to dedicate good agents and analysts to these prosecutions?

Response:

Any civil rights complaint that appears on its face to be a violation of federal criminal law must be opened and investigated. The results of civil rights investigations are submitted to DOJ and the USAO for a prosecutorial opinion. It is the prosecutor's responsibility to decide whether the case merits prosecution. The premise of the question, that the number of Agents working civil rights investigations is rapidly declining, is not accurate. While there was a dramatic decrease immediately following the events of 9/11/01, these numbers are beginning to increase. In addition, the Civil Rights Program (CRP) is among the FBI's top 10 priorities, and appropriate resources have been allocated to the program. It is the responsibility of each field division's Special Agent in Charge (SAC) to ensure that these resources are employed according to the FBI's and the field division's priorities. At least three in-service training sessions are conducted by the CRU annually to ensure that all those working civil rights matters receive adequate training. When needed, additional training is provided.

53. (Follow-up to Leahy 11) It appears that of the two freedom of access to clinics matters, one was instituted by the prior Administration. Thus, there has been only one freedom of access prosecution since President Bush took office. How many reports alleging possible violations of FACE were received in this time frame, and how many investigations were referred for prosecution? What is the status of the government appeal in U.S. v. Bird?

Response:

The below chart reflects the number of Freedom of Access to Clinic Entrances (FACE) Act investigations the FBI has initiated and the number of federal indictments, arrests, and convictions obtained beginning in FY 2001.

FY	FACE Cases Initiated	Federal Indictments	Federal Arrests	Federal Convictions
2001	42	0	0	1
2002	23	0	1	1
2003	20	2	1	1
2004 (thru end of 2d qtr)	9	0	0	0

As reflected by the steady decline in case initiations, traditional FACE Act incidents (such as telephone threats and vandalism) have declined since their peak in the 1990s. While this decline has been observed by both law enforcement and non-governmental organizations (NGOs) alike, matters that fall within the FACE subprogram often overlap with other FBI programs and are classified with those programs. For example, FACE investigations involving bio-terrorism threats to reproductive health care facilities (such as letters threatening to contain anthrax) previously investigated as FACE Act violations are now opened as terrorism matters. Similarly, a bombing at a reproductive health care facility where organized hate groups are believed to be involved may be classified as a domestic terrorism matter.

As indicated above, civil rights investigations are subject to a greater level of routine outside scrutiny than most investigations; unlike other FBI criminal programs, the results of all civil rights investigations, to include FACE matters, are provided to DOJ and the local USAO for review.

The case of United States v. Bird arises from an incident on 3/7/03, when Bird drove a vehicle into the entrance of a Planned Parenthood building in Houston, Texas. In August 2003, a United States District Court ruled that the Commerce Clause of the FACE Act, under which Bird was indicted, was unconstitutional.

DOJ has appealed this ruling to the 5th Circuit Court of Appeals, and briefs have been filed. A hearing date has not yet been set.

54. (Follow-up to Leahy 11) Based on the summaries you provided, it appears that only 9 prosecutions involving the FBI as the lead investigative agency were hate crimes directly related to the events of September 11, 2001. Is that correct? How many complaints did the FBI receive following September 11, 2001, that involved possible violations in the "Hate Crime" category of cases you described?

Response:

As indicated above, any civil rights complaint that appears on its face to be a violation of federal civil rights law is opened and investigated thoroughly. While the FBI maintains statistics on hate crimes, it does not maintain statistics on the number of civil rights complaints received, and the specific number of hate crimes apparently committed in retaliation for the attacks of 9/11/01 is unknown. Between 9/11/01 and June of 2004, approximately 531 hate crime investigations were initiated in which it appeared that Arabs, Muslims, or Sikhs were targeted. Because there may be a delay between the filing of an allegation (particularly when it is lodged with an entity outside the FBI), the initiation of the investigation in the field, and the field's report to FBIHQ, this number may not be a true reflection of the total number of such cases. Of the reported 531 investigations, 13 cases resulted in 18 subjects being charged federally, and another 178 subjects were charged on the local level. Because these cases are typically worked jointly between local law enforcement officials and the FBI, local prosecutions often proceed before federal cases are brought. In cases in which the federal interest has been satisfied by a successful local prosecution, the federal government may choose not to pursue an additional conviction. The federal prosecutor's decision not to proceed with a prosecution in no way reflects on the quality of the FBI's investigation.

55. (Follow-up to Leahy 15) What specific policy changes have you made in response to the Inspector General's report on 9/11 detainees?

Response:

DOJ and DHS have signed an MOU relating to information sharing, and the FBI is working with others in DOJ to draft an MOU governing the detention of aliens of interest to the FBI. In addition, DOJ is working with DHS to draft an MOU establishing criteria and procedures for future investigations of alien detainees of national security interest. The FBI has also worked to establish the Terrorist Screening Center (TSC) and to assist in establishment of TTIC, which will substantially improve the FBI's ability to obtain information about alien detainees from various agencies and to process this information in a timely fashion. The

FBI continues to work with the National Security Law Division of DHS Immigration and Customs Enforcement (ICE) to review alien detainee cases of national security interest on a case-by-case basis.

56. (Follow-up to Leahy 16C) Has a final decision been made as to whether prior approval is mandatory for visiting a public place or attending a public event to detect or prevent terrorist activity?

Response:

The policy regarding attendance at public events and places is articulated in Part VI of the revised Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations (General Crimes Guidelines). In implementing this guidance, FBI policy provides that a supervisor's approval is recommended but not required. There are no current plans to change this policy, because there has been no indication that the authority has been misused or that greater oversight is needed for any other reason. Should these circumstances change, the need for greater oversight will be re-evaluated.

Part VI of the General Crimes Guidelines is only one of several authorities governing attendance at public events or visitation of public places. Agents may also engage in these activities as part of a full field investigation or a preliminary inquiry under the General Crimes Guidelines or appropriate provisions of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection. (NSIG). Since internal FBI policy requires that international terrorism investigations be conducted pursuant to the NSIG, attendance at public places and events to detect or prevent international terrorism would typically be authorized under those guidelines.

57. (Follow-up to Leahy 17) Why didn't the FBI participate in the review of the 4,500 intelligence files? To your knowledge, did the FBI receive any referrals from DOJ based on this review? If so, please provide details to the extent possible (without jeopardizing a current investigation).

Response:

The review of intelligence files was undertaken at the direction of the Attorney General specifically to enable criminal prosecutors to identify and evaluate information in intelligence files which prosecutors found appropriate for criminal investigation. These files had been developed by FBI agents, many of whom had been involved only in intelligence investigations and had no experience in criminal investigations. Turning a prosecutor's eye on this information was the precise purpose of this review. The FBI fully cooperated with this review, making files available and responding to questions as needed. Following this

review, the FBI, working in conjunction with prosecutors, conducted further investigation where appropriate with an eye to developing criminal cases. More than 500 criminal investigations were initiated following the file review, some of which have resulted in prosecutions.

58. (Follow-up to Leahy 18A) When will the FISA Management System (FISAMS) be fully operational? With whom is the contract for development of FISAMS? How much will it cost and what funds are being used to pay for it?

Response:

The FISA Management System (FISAMS) became operational at the end of January 2004. The FBI has trained the largest 13 FBI field offices on the system. These 13 offices are currently processing their FISA requests, which account for approximately 75% of FBI FISAs, through the FISAMS. The remaining FBI field offices are in the process of being trained, and all FBI offices will be operational in the FISAMS by the end of CY 2004.

High Performance Technologies, Inc. (HPTi) is the contractor responsible for development of the FISAMS. The FBI allocated $900,000 for Version 1.0 of the FISAMS in FY 2003, and is contracting with HPTi for an additional $1 million in enhancements, funded by the Wartime Supplemental appropriation, beginning in the fall of 2004. While several follow-up versions are anticipated to further enhance FISAMS in the future, FY 2006 is the first budget cycle in which targeted funding for this project has been requested.

59. (Follow-up to Leahy 18C) Did you personally review the 4 FISA applications reportedly not approved by the FISA court last year? Can you provide any details on why the 4 applications were not approved?

Response:

The Director of the FBI personally certifies each FISA application submitted to him. Details about the four applications were provided in the Department's highly classified, statutorily mandated semi-annual report on the FISA process, "The Attorney General's Report on Electronic Surveillance and Physical Search under the Foreign Intelligence Surveillance Act," for the reporting period in which those applications were presented to the Foreign Intelligence Surveillance Court. That report was filed with the Senate Select Committee on Intelligence and access to it by other appropriately cleared Senate staff may be obtained in coordination with that committee.

60. (Follow-up to Leahy 18D) Can you provide us with a blank copy of the FISA Request Form referenced in your response? Will you provide us with a blank copy of the form that the FBI created for requesting business records from the FISA court?

Response:

This response is classified and is, therefore, provided separately.

61. (Follow-up to Leahy 21) Did you refer the question to DOJ OIPR? When? Have you been asked to assist in the response? When?

Response:

The FBI forwarded its response to Senator Leahy's question 21 to DOJ on 10/22/03, indicating that the question called for classified information that is ordinarily supplied to Congress by DOJ's Office of Intelligence Policy and Review (OIPR). By letter to the Committee dated 3/4/04, DOJ's Office of Legislative Affairs forwarded the responses to the Committee, which included the FBI's original response to this question in which the FBI deferred to OIPR as the more appropriate component to whom the Committee should direct such questions.

62. (Follow-up to Leahy 22) Can you provide a copy of the "collection baseline that defines the sum total of resources the FBI can bring to bear on a given threat" when it is completed (estimated mid-November 2004?) to respond to the "connect the dots" issue? Have you yet identified gaps in your knowledge about threats? How can Congress help to ensure there are no such gaps?

Response:

The collection baseline is a large database and, consequently, providing a copy is problematic. In addition, the baseline tool, data, and the reports that can be generated cannot be fully understood without contextual knowledge. The FBI would be pleased to provide a classified briefing and demonstration of the baseline.

The FBI's collection baseline tool allows us to "know what we could know," and the work to identify what we don't know (i.e., the work to identify gaps) continues. Once gaps are identified, the FBI develops collection strategies to fill those gaps through a variety of intelligence collection methods. There will always be gaps in any intelligence organization's knowledge about threats. The key to the FBI's success is the creation of an independent entity, the Intelligence Requirements and Collection Management Unit, that focuses full time on identifying gaps and developing strategies for filling them. The FBI understands

its responsibility to ensure customers and stakeholders are aware of collection gaps and are confident in the FBI's plans to fill them, and we would be pleased to provide Congress with classified briefings on the status of FBI intelligence collection capabilities.

The FBI appreciates the support Congress has demonstrated by providing resources and legislation to strengthen the FBI's ability to protect the American public and U.S. interests around the world. We would appreciate your continued support with respect to our plans for a robust intelligence capability in the FBI, especially in the areas of Intelligence Analyst staffing and retention; intelligence training; and information technology support for our intelligence activities, including the infrastructure improvements needed to support secure information networks.

63. (Follow-up to Leahy 31) Is TTIC the "one place" where all terrorism-related information is brought together? How is such information disseminated (*e.g.* through email, a website, faxes, telexes, etc.)?

Response:

The NCTC (formerly TTIC) serves as the organization in the U.S. Government (USG) primarily responsible for analyzing intelligence pertaining to terrorism that is possessed or acquired by the USG (except purely domestic terrorism). Although the NCTC has primary responsibility for terrorism threat analysis, a number of organizations throughout the federal government have been assigned responsibilities with respect to terrorism information by statute, Presidential Directive, regulation, and policy. These include primarily the CIA, FBI, and DHS. In addition, the Departments of State, Defense, Treasury, and numerous others analyze the terrorist threat from their particular perspectives.

Among other means, the NCTC's terrorism threat analysis is disseminated by the FBI, DHS, and other federal officials assigned to this interagency organization, who push threat information out to state and local officials and law enforcement personnel through the JTTFs, state emergency management agencies, and other organizations operating at the state and local level. In addition, NCTC uses production and dissemination mechanisms that are commonly employed in the federal government based on customer needs and their communication technology capabilities, including classified and unclassified faxes, hard copy dissemination, and cables. Because NCTC is mindful of the need to produce intelligence information at the lowest possible classification level in order to ensure that it reaches the widest possible audience, it frequently prepares reports on a given subject at multiple classification levels. This ensures that the dissemination of important information is not delayed by the need to declassify intelligence.

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

64. (Follow-up to Leahy 32) Please answer the question asked: Were there other instances directly or indirectly connected with the September 11 attacks where, because of the "perception" within the FBI that the "FISA process was lengthy and fraught with peril," investigative avenues were not pursued? Please describe any such instance where FISA was considered but not used.

Response:

The FBI is aware of no instances directly or indirectly connected with the 9/11 attacks in which a FISA was considered but not pursued because of the nature of the FISA process.

65. (Follow-up to Leahy 33) What financial support networks have been "closed down" using the PATRIOT Act? Please describe your efforts and results in detail.

Response:

The USA PATRIOT Act has provided the means to disrupt terrorist financial support networks. The FBI has used the USA PATRIOT Act to pursue several significant investigations throughout the U.S. Given the global nature of financial support networks, the actual "closure" of a financial support network can only be achieved with complete international cooperation. Through the United Nations' designation process, which triggers international obligations on the part of all member countries with regard to individuals and entities associated with the Taliban, Usama bin Laden, or al Qaeda, several corrupt nongovernmental organizations (NGOs), such as charities ostensibly operating to provide humanitarian aid, have been blocked from transmitting or receiving money, goods, services, or other material support. The designation process requires member nations to take affirmative steps to ensure that designated organizations and individuals cannot use their remaining infrastructure or finances to fund or otherwise support terrorism. The public identification of terrorists, terrorist organizations, and terrorist supporters assists in terminating their activities, since this prohibits other entities from having dealings with them.

These blocking actions are critical to combating the financing of terrorism. When a blocking action is put into place, any property – including assets -- that exists in the U.S. is frozen, and U.S. persons and persons within the jurisdiction of the United States are prohibited from transacting or dealing with individuals and entities who are the subject of the blocking action. Blocking actions serve additional functions as well, including serving as a deterrent for nondesignated parties who might otherwise be willing to finance terrorist activity; exposing

terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers; disrupting terrorist financing networks by encouraging designated terrorist supporters to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups; terminating terrorist cash flows by shutting down the pipelines used to move terrorist related assets; forcing terrorists to use alternative, more costly, and riskier means of financing their activities; and engendering international cooperation and compliance with obligations under U.N. Security Council Resolutions. To date, the United States and our international partners have designated 368 individuals and organizations as terrorists and terrorist supporters and have frozen approximately $139 million and seized more than $60 million in terrorist related assets.

A notable disruption of an NGO using the USA PATRIOT Act's material support statutes was effected through the investigation of the United States office of the Benevolence International Foundation (BIF) in Chicago, Illinois. The chairman of BIF ultimately pled guilty to a lesser charge and the BIF office closed.

Also of note is the series of actions taken against the umbrella charities of the Al-Haramain Foundation (AHF). Before the removal of the Taliban from power in Afghanistan, the AHF in Pakistan supported the Taliban and other fundamentalist groups. AHF was linked to the UBL-financed terrorist organization, Makhtab al Khidemat (MK). On one occasion in 2000, MK directed the deposit of funds in AHF accounts in Pakistan and, from there, the transfer of these funds to other accounts. At least two former AHF employees who worked in Pakistan are suspected of having al Qaeda ties. One AHF employee in Pakistan is detained at Guantanamo Bay on suspicion of financing al Qaeda operations. Another former AHF employee in Islamabad was identified as an alleged al Qaeda member who reportedly planned to carry out several devastating terrorist operations in the United States.

A search warrant was executed in 2004 at the United States branch of the AHF in Ashland, Oregon. The search was led by Agents of the Internal Revenue Service Criminal Investigations section as part of a joint FBI/DHS (ICE) investigation into possible violations of the Internal Revenue Code, the Money Laundering Control Act, and the Bank Secrecy Act. The suspected crimes relate to possible violations of the currency reporting and tax return laws by two officers of the Ashland, Oregon, office of AHF. In a separate administrative action, based in large part on a JTTF investigation, the Department of Treasury Office of Foreign Assets Control (OFAC) blocked AHF accounts to ensure the preservation of its assets pending further OFAC investigation.

In March 2002, the Department of Treasury and the Kingdom of Saudi Arabia jointly designated the Bosnian and Somalian Branches of AHF as supporters of

terrorism. In December 2003, the reconstituted branch of AHF in Bosnia, now called Vazir, was also designated by both governments as a supporter of terrorism. In January 2004 these two governments also jointly designated AHF branches in four additional countries as being supporters of terrorism: Indonesia, Tanzania, Kenya, and Pakistan. The United Nations has adopted these AHF designations and imposed asset freezes, travel bans, and arms embargoes pursuant to United Nations Security Council Resolutions.

The AHF activities resulting in these sanctions took place under the control of Aqeel Abdulaziz Al Aqil, the founder and longtime leader of AHF and a suspected al Qaeda supporter. Al Aqil has been identified as AHF's Chairman, Director General, and President by a variety of sources and reports. Having been under investigation since late 2003, by March 2004 Al Aqil was reportedly no longer leading AHF activities. Under Al Aqil's leadership, numerous AHF field offices and representatives operating throughout Africa, Asia, Europe, and North America appear to have provided financial and material support to the al Qaeda network. Terrorist organizations designated by the U.S., including Jemmah Islammiya, Al Ittihad Al Islamiya, Egyptian Islamic Jihad, HAMAS, and Lashkar E Taibah, have received funding from AHF and have used AHF as a front for fund raising and operational activities. AHF has offices and representatives in more than 50 countries and includes nine general committees and several other "active committees," including the Continuous Charity Committee, African Committee, Asian Committee, Da'wah and Sponsorship Committee, Masjid Committee, Seasonal Projects Committee, Doctor's Committee, European Committee, Internet and the American Committee, the Domestic Committee, Zakaat Committee, and the Worldwide Revenue Promotion Committee. On 6/3/04 the USG announced the joint Saudi-U.S. designation of five AHF offices: Afghanistan, Albania, Bangladesh, Ethiopia, and the Netherlands. The USG independently designated Al-Aqil, the former head of AHF operations in Saudi Arabia.

In addition, the USG has designated other NGOs which support terrorist-related activities, including:

Makhtab al Khidamat/Al Kifah (formerly based in the U.S.)
Al Rashid Trust (Pakistan)
WAFA Humanitarian Organization (Pakistan, Saudi Arabia, Kuwait, and UAE)
Rabita Trust (Pakistan)
The Holy Land Foundation for Relief and Development (U.S.)
Ummah Tamer E Nau (Pakistan)
Revival of Islamic Heritage Society (Kuwait, Afghanistan, and Pakistan)
Afghan Support Committee (Pakistan)
Aid Organization of the Ulema (Pakistan)
Global Relief Foundation (U.S.)

Benevolence International Foundation (U.S.)
Benevolence International Fund (Canada)
Bosanska Idealna Futura (Bosnia)
Lajnat al Daawa al Islamiyya (Kuwait)
Stichting Benevolence International Nederland (Netherlands)
Al Aqsa Foundation (U.S., Europe, Pakistan, Yemen, and South Africa)
Comité de Bienfaisance et de Secours aux Palestiniens (France)
Association de Secours Palestinien (Switzerland)
Interpal (UK)
Palestinian Association in Austria (Austria)
Sanibil Association for Relief and Development (Lebanon)
Al Akhtar Trust (Pakistan)
Islamic African Relief Agency (U.S., Sudan)

66. (Follow-up to Leahy 34B) Has the FBI implemented any new professional rules of conduct or code of ethics policies that provide safeguards against FBI abuse of its PATRIOT Act authorities? What, if any, internal or disciplinary punishments are in place for abuses by employees?

Response:

The FBI's existing rules of professional conduct, which require Agents to uphold the Constitution and to adhere to the highest standards of personal and professional behavior, safeguard against the abuse of USA PATRIOT Act provisions. For the most part, the USA PATRIOT Act provisions relevant to the FBI's mission amend existing federal investigative processes (e.g., search warrants) for which there is, in varying degrees, oversight by the executive, judicial, or legislative branches of government, or a combination thereof. For example, most FBI activities pursuant to FISA require approval by the DOJ Office of Intelligence Policy and Review and the FISA Court. Similarly, delayed notice search warrants and search warrants for voice mail must be approved by a U.S. District Court. As another example, requests for bank account information under Section 314 of the USA PATRIOT Act require approval by the Treasury Department's Financial Crimes Enforcement Network (FinCEN). Other provisions, such as Section 215, require annual reports to the Congress. In addition to these checks on abuse, information sharing must be conducted in compliance with the Privacy Act of 1974 and with various internal policies that ensure Privacy Act compliance, such as those promulgated by the FBI's Privacy Council. For example, the Privacy Act prohibits the collection and maintenance of record information about individuals based solely on the exercise of their First Amendment rights. In sum, there is already in place a network of checks and balances which will operate to guard against abuse and, if abuse does occur, to detect and correct it.

If abuse should occur, it would be addressed through the FBI's disciplinary process, which is overseen by the FBI's Office of Professional Responsibility (OPR) and the DOJ OIG. The OPR/OIG process aggressively and impartially addresses allegations of employee misconduct, including alleged violations of individuals' Constitutional or statutory rights, ensuring that the FBI maintains its integrity and professionalism. In addition, each FBI field office is inspected every three years for compliance with rules and regulations by the Inspection Division.

The FBI also ensures that Agents are trained to respect the Constitutional rights of individuals through extensive instruction on Constitutional law and criminal procedure and guidance on the importance of sensitivity to other cultures. As part of this training, new Agents also visit the Holocaust Museum so that they can see, graphically, what can occur when law enforcement becomes a tool for oppression.

67. (Follow-up to Leahy 35) Have you seen an "increase" in global computer hacking activities in either the United States or Iraq because of growing tensions between the two countries? Please explain your answer.

Response:

The FBI is unable to attribute any change in global computer hacking activities to the relationship between the United States and Iraq.

68. (Follow-up to Leahy 36) Will you provide a response to Leahy 36 in a classified document and submit it for review by appropriate staff? Why did you not just submit the response in classified form as you have done on other occasions?

Response:

The FBI was not directed to develop the referenced guidelines and defers to the Administration with respect to the existence or status of such guidelines.

69. (Follow-up to Leahy 37) Please provide details on the "successful disruptions" of al Qaeda financing operations that have been accomplished? Have there been any indictments brought, informations filed, or convictions obtained as a result of the Joint Saudi Financial Investigative Unit? Please explain your answer.

Response:

The joint USG-Saudi task force, known as the Joint Task Force on Terrorist Finance (JTFTF), has been in operation for less than a year. Information obtained thus far has been folded into several other CT and criminal investigations which

have yet to reach the indictment stage. Valuable information continues to be exchanged with respect to CT matters and classified intelligence investigations.

Questions Posed by Senator Kennedy

70. On May 13, 2004, the *New York Times* reported that the Central Intelligence Agency has used a variety of coercive intelligence methods, including a technique known as "water boarding," against certain terrorist suspects. It stated that these rules for interrogation have been endorsed by the Justice Department and the C.I.A. The *Times* further reported: "The methods employed by the C.I.A. are so severe that senior officials of the Federal Bureau of Investigation have directed its agents to stay out of many of the interviews of the high-level detainees, counterterrorism officials said. The F.B.I. officials have advised the bureau's director, Robert S. Mueller III, that the interrogation techniques, which would be prohibited in criminal cases, could compromise their agents in future criminal cases, the counterterrorism officials said."

a. Please provide a copy of these rules for interrogation.

b. Who at the Justice Department approved these rules of interrogation? Please provide all documentation pertaining to their proposal, consideration, and approval.

Response to a and b:

The FBI defers to DOJ with respect to these questions.

c. Which officials at the FBI told you about the rules of interrogation, and who informed you that they might compromise your efforts to prosecute suspected terrorists? Did these officials or any other official at the Justice Department provide an opinion as to the legality of these methods? Please provide a copy of every legal opinion you have received on this issue.

d. The *New York Times* reported that one set of legal memorandums prepared by the C.I.A. and the Justice Department "advises government officials that if they are contemplating procedures that may put them in violation of American statutes that prohibit torture, degrading treatment or the Geneva Conventions, they will not be responsible if it can be argued that the detainees are formally in the custody of another country." Are you familiar with this legal opinion? Do you agree with it? Has the FBI participated in any effort to place a detainee in the arguable "formal custody" of another country so that more severe interrogation methods may be used?

Response to c and d:

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

e. Since 9/11, there have been multiple reports about detainees in the custody of U.S. military or intelligence officials being transferred for interrogation to governments that routinely torture prisoners. A December 2002 article in the *Washington Post* reported that detainees who refuse to cooperate with American interrogators have been "rendered" to foreign intelligence services known to practice torture. The Convention Against Torture – to which the United States is a party – provides that "No State Party shall expel, return or extradite a person to another State where there are substantial grounds for believing he would be in danger of being subjected to torture." Can you assure the Committee that the FBI has fully complied with this legal requirement and not participated in any way in any "renditions" of detainees to countries known to practice torture?

Response:

Consistent with Article 3 of the Convention Against Torture as ratified by the United States, the FBI has not transferred custody of any detainee to a country where it is more likely than not that the detainee would be subject to torture.

71. Last year the Attorney General announced that information regarding more than 400,000 persons with removal orders and an unknown number of alleged NSEERS violators would be included in the NCIC database. As you know, these are cases of persons with administrative warrants, not criminal warrants. What is the legal authority for the FBI to enter administrative warrants into its principal criminal law database? What other immigration-related records does the Administration plan to include in NCIC? Are there any restrictions regarding the type of cases that can be entered into NCIC?

Response:

The authority of the Attorney General to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records is provided by 28 U.S.C. 534. Pursuant to this authority, which is exercised within DOJ by the FBI, many of these records are obtained from state and local criminal justice agencies and managed by the FBI, which serves as the national focal point and central repository for criminal justice information records. In addition, 8 U.S.C. 1252c(a) provides that "[s]tate and local law enforcement officials are authorized to arrest and detain an individual who - (1) is an alien illegally present in the United States; and (2) has previously been convicted of a felony in the United States and deported or left the United States after such conviction, but only after the State or local law enforcement officials obtain appropriate confirmation from the Immigration and Naturalization Service of the status of such individual and only for such period of time as may be required for the Service to take the individual into Federal custody for purposes of deporting or removing the alien from the United States."

8 U.S.C. 1252c(b) requires that the Attorney General "cooperate with the States to assure that information in the control of the Attorney General, including information in the National Crime Information Center, that would assist State and local law enforcement officials in carrying out duties under subsection (a) of this section is made available to such officials." In satisfaction of this requirement, and under the authority afforded by 28 U.S.C. 534, the Attorney General promulgated 28 Code of Federal Regulations (C.F.R.), Part 20. 28 C.F.R. 20.32 defines the offenses includable in criminal history records as follows.

> (a) Criminal history record information maintained in the III System and the FIRS [Fingerprint Identification Records Systems] shall include serious and/or significant adult and juvenile offenses.
>
> (b) The FIRS excludes arrests and court actions concerning nonserious offenses, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, and traffic violations (except data will be included on arrests for vehicular manslaughter, driving under the influence of drugs or liquor, and hit and run), when unaccompanied by a § 20.32(a) offense. These exclusions may not be applicable to criminal history records maintained in state criminal history record repositories, including those states participating in the NFF.
>
> (c) The exclusions enumerated above shall not apply to federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of this subpart.

In December 2003, the FBI's Criminal Justice Information Services Division (CJIS) Advisory Policy Board (APB) considered the inclusion of Student and Exchange Visitors Information System violators and non-felony deported aliens in the NCIC Immigration Violator File (IVF). Although the addition of these two categories of information was approved in concept, implementation must be delayed until:

- These actions are supported by criminal warrants;
- This change is directed by appropriate authority; or
- These actions can be documented in an "information only" file with acceptable caveats.

This is the only proposed addition of which the FBI is aware.

72. The error rate in immigration records has always been very high. Numerous reports by the Inspector General of DOJ have confirmed the unreliability of INS records. What precautions are being taken to ensure that the immigration records being put into NCIC are accurate so that persons with legal status are not falsely arrested as a result of an inaccurate entry? What mechanism exists for updating and correcting information in the NCIC database?

Response:

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. A record may be modified only by the agency that entered the record. ICE's Law Enforcement Support Center (LESC) is the only entity that can enter records into the NCIC IVF, and it must comply with all NCIC policies. The following information, provided by ICE, describes the steps ICE takes to comply with NCIC policies.

NCIC policies require that every record entered be based on a valid original source document. For deported felons, that document is an executed warrant of removal; for alien absconders it is a warrant of removal; and for National Security Entry-Exit Registration System violators it is an administrative warrant of arrest. NCIC policies require that hit confirmation be conducted 24 hours a day, seven days a week, and within ten minutes. To meet the ten minute response time requirement, the LESC maintains fingerprints and photographs, as well as the original documentation to support a record's entry in the NCIC IVF.

The LESC reviews each alien file to determine if a record should be entered in one of the IVF categories. These reviews involve comprehensive research of the source documents and electronic data contained in the separate ICE databases to ensure data integrity and suitability for an NCIC entry.

Additionally, validation procedures exist to ensure that accurate records are entered into NCIC. Validation obliges the LESC to confirm that the record is complete, accurate, and still outstanding or active. IVF records must be validated 60 to 90 days after entry and every year thereafter. Validation is accomplished by reviewing the original entry and current supporting documents.

As the manager of NCIC, the FBI helps maintain the integrity of the system through: 1) automatic computer edits which reject certain common types of errors in data, 2) automatic purging of records after they are in a file for a prescribed period of time, 3) quality control checks by the FBI's Data Integrity staff, and 4) periodically furnishing lists of all records on file for validation by the agencies that entered them.

Each federal and state CJIS System Agency is audited at least once every three years by the FBI's audit staff. This audit includes a sample of state and local criminal justice agencies and their records. The objective of this audit is to verify adherence to FBI policies and regulations, and is termed a compliance audit. The FBI audit staff also conducted an informational NCIC audit of LESC in August 2003. Since the LESC acquired sole responsibility over the entry and maintenance of the NCIC IVF, there has been an improvement in the validity, accuracy, and completeness of both the records and the supporting documentation.

73. The CLEAR Act would require that records of minor immigration violators be included in NCIC. This bill is opposed by many law enforcement agencies around the country. This particular provision in the bill was soundly criticized last month by the conservative Heritage Foundation, which stated that this mandate "may hinder law enforcement by undermining the usefulness" of the NCIC database. The report further states: "Filling the database with records of minor immigration violators could also distract or impede police officers from using the database to obtain information about violent criminals and terrorists." The report concludes that "NCIC should be reserved for serious, significant immigration violations." What is your view of the conclusions reached by the Heritage Foundation? Can we afford to jeopardize the integrity of the NCIC database?

Response:

The main issue of concern for the law enforcement community, as voiced through the CJIS APB, has been the authority to arrest immigration violators. The law enforcement community does not want to retrieve records from NCIC with respect to individuals on whom they can take no action. The inclusion of immigration violators in NCIC and local law enforcement's right of arrest are currently the basis of a lawsuit filed by the American Civil Liberties Union.

74. In June 2003, Glenn Fine, the Inspector General for the Justice Department, found "significant problems in the way the detainees were handled" following 9/11. These problems included a failure by the FBI to distinguish between detainees whom it suspected of having a connection to terrorism and detainees with no connection to terrorism; the inhumane treatment of the detainees at a federal detention center in Brooklyn; and the unnecessarily prolonged detention resulting from the Department's "hold until cleared" policy – made worse by the FBI's failure to give sufficient priority to carrying out clearance investigations. In your opinion, has the Justice Department responded in an appropriate manner to all the abuses identified in the Inspector General's report? What steps has the FBI taken to prevent such abuses from occurring in the future?

Response:

The FBI worked diligently to determine whether the detainees, all of whom were in the United States illegally, did, in fact, have terrorism connections. When the FBI was able to determine that an alien was not of interest to the 9/11 investigation, the immigration authorities were notified as soon as possible. While many of the investigations of detainees took some time, for reasons discussed in the Inspector General's report, thorough investigation was necessary to ensure that these detainees posed no danger to our national security.

Several steps have been taken to ensure that future detainee matters are handled as efficiently and effectively as possible. As the Acting Deputy Attorney General explained in his 11/20/03 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). For example, an effort is underway to prepare an MOU between DHS and DOJ regarding criteria and procedures for identifying alien detainees of national security interest. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and to work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other initiatives, such as the Foreign Terrorist Tracking Task Force (FTTTF) and the National Joint Terrorism Task Force (NJTTF), have enhanced the flow of information with our law enforcement counterparts and will improve the handling of such cases.

75. Enacted in 1990, the Hate Crime Statistics Act (HCSA) requires the Justice Department to acquire data on crimes which "manifest prejudice based on race, religion, sexual orientation, disability, or ethnicity" from law enforcement agencies across the country and to publish an annual summary of the findings. The HCSA, implemented by the FBI as part of its Uniform Crime Reporting (UCR) Program, now provides the best national picture of the magnitude of the hate violence problem in America – though it is still clearly incomplete.

On November 12, 2003, the FBI released its annual report, *Hate Crime Statistics 2002*, of data collected under the HCSA. The FBI documented 7,462 hate crime incidents: 48.8% based on racial bias, 19.1% based on religious bias, 16.7% based on sexual orientation bias, and 14.8% based on ethnicity bias. The number of national law enforcement agencies reporting to the FBI in 2002 increased slightly from 11,987 to 12,073: the second highest total of participating agencies in the twelve-year history of the data collection effort. However, of the 12,073 agencies that participated, only 1,868 agencies (15.5%) reported even a single hate crime, a slight increase from the 17.6% that reported incidents in 2001. Thus, for 2002, 10,205 agencies (84.5%) reported *zero* hate crimes.

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

Response:

The FBI recognizes the importance of meaningful training to an individual's ability to perform effectively. Such training benefits state and local law enforcement agencies' recognition of hate crimes, which in turn assists the Uniform Crime Reporting (UCR) Program in identifying the magnitude of the problem nationwide. Over the last 4 fiscal years, the FBI's UCR Program has provided hate crime training to 1,857 law enforcement personnel during 38 training sessions in over 20 states and the District of Columbia. Year-by-year figures are as follows.

Fiscal Year	Number of Training Sessions	Number of States in Which Training was Conducted	Number of Agencies Represented	Number of Persons Trained
2001	14	8 + D.C.	438	771
2002	18	10	249	498
2003	4	3	366	577
2004 (9 months)	2	2	5	11

Face-to-face training sessions typically last 4-6 hours and include potential elements of bias motivation, how to identify the types of bias motivation for which the national UCR Program is required to collect data, and how to properly score and report an incident depending on the agency's reporting method (i.e., the Summary reporting system or the National Incident-Based Reporting System (NIBRS)).

The FBI also recognizes that, because of work schedules, location, budget restrictions, and a host of other factors, training is not always easy to obtain. Consequently, the UCR Program worked more than 2 years to develop and test effective Web-based hate crime identification and scoring training, which became available on the Law Enforcement OnLine (LEO) intranet in the summer of 2002. The FBI encourages those agencies wanting hate crime training to explore this Web-based option for their officers on LEO at: http://home.leo.gov/lesig/cjis/programs/crime_statistics/hate_crime_web_training/. (The access path from the LEO Home Page is LEOSIGs | CJIS | Programs | Uniform Crime Reporting | Hate Crime Web Training.) Law enforcement personnel requiring a LEO application may call the LEO Help Desk at 888-334-4536. The recent decrease in training is attributable both to the availability of this on-line training and to a temporary

reduction in training while the FBI uses those resources to develop the Law Enforcement National Data Exchange (N-DEx) Program, the purpose of which is the development of an improved, more useful UCR program. Although the FBI needed to commit the skills of those experienced in UCR to the development of N-DEx, N-DEx will substantially enhance the FBI's ability to provide hate crime information. The FBI is developing the training requirements necessary to implement the N-DEx Program and to ensure common reporting standards are achieved. Training will be incorporated into the N-DEx curriculum to improve Hate Crimes reporting through this process.

In addition to the above UCR Program training, the FBI's CRU and 56 FBI Field Offices routinely provide training to local and state law enforcement agencies regarding civil rights matters, including hate crimes. Hate crime training is also provided in quarterly National Academy (NA) courses, attended by specially nominated and selected representatives of state, local, and international law enforcement agencies. Approximately 1,000 NA attendees receive this training annually, enabling them to provide instruction to their respective departments.

b. What steps is the FBI taking to increase participation in the HCSA data collection effort?

Response:

In addition to the face-to-face and Web-based courses geared specifically to hate crime instruction, the national UCR Program briefs law enforcement personnel with respect to the hate crime data collection effort in its mainstream UCR training for Summary reporting and for NIBRS training. The FBI also keeps state UCR Programs and direct contributors informed of hate crime reporting procedures and training opportunities via the UCR *State Program Bulletin* and *UCR Newsletter*, respectively.

c. Excellent FBI training materials on how to identify, report, and respond to hate crime are now available online: http://www.fbi.gov/ucr/traingd99.pdf and http://www.fbi.gov/ucr/hatecrime.pdf. Are there any plans to update these 1999 resources to better reflect post-9/11 realities?

Response:

The FBI periodically updates all of its training materials. The update of both *Hate Crime Data Collection Guidelines* and *Hate Crime Training Guide* will include post-9/11 realities.

76. Professor Jack McDevitt, Director of The Center for Criminal Justice Policy Research at Northeastern University in Boston, has 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, Professor McDevitt suggested that more detailed reporting can reduce the occurrence of "information disconnect" between the investigating officer and UCR reporting officials. Do you agree that the FBI's Hate Crime Incident Report forms should be revised to provide space to encourage additional narrative about the bias motivation present?

Response:

Because participation in the UCR Program is voluntary, it would be counterproductive to participation to impose additional reporting burdens on law enforcement. In 2002, for example, law enforcement officers would have been required to write narratives concerning 7,462 hate crime incidents. Though the information collected from the Hate Crime Incident Report is somewhat limited, the FBI is able to collect more comprehensive data about hate crimes (and a wider scope of crime in general) from agencies that report crime using the 56 data elements of the NIBRS. The FBI is involved in an extensive national effort to redevelop and automate the UCR Program to enhance hate crime reporting.

77. 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 that had hate crime laws included gender. Today, including the District of Columbia, twenty-eight of the forty-seven 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 also subject to Federal sentencing enhancements under 28 U.S.C. § 994. Do you share my view that the FBI's Hate Crime Incident Report should include a box in the Bias Motivation section for gender-based hate crimes? Is there some legal impediment to making that change, or could the Bureau take this step on its own?

Response:

The FBI's UCR Program was assigned the task of collecting hate crime data according to the specific bias motivations stipulated in various hate crime statutes. The 1990 Hate Crime Statistics Act (HCSA) mandated a 4-year collection of data regarding biases against race, religion, sexual orientation, and ethnicity. In September 1994, the Violent Crime Control and Law Enforcement Act amended the HCSA to add bias against disabilities. Subsequently, the Church Arson Prevention Act of 1996 amended the collection duration to require collection "for

each calendar year," making the data collection effort a permanent part of the UCR Program. Should future legislation mandate the collection of gender-biased hate crimes, the FBI would comply.

78. 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" directed at individuals in the aftermath of the September 11th terrorist attacks, wouldn't the FBI benefit from including on its form at least one additional box for "Anti-Arab" crimes?

Response:

Though early hate crime data collection criteria included a code to indicate Anti-Arab as a subcategory of Ethnicity/National-Origin Bias, the code became invalid in 1996 as a result of changes from the Office of Management and Budget (OMB) concerning the administrative reporting of statistics as they pertain to race and ethnicity. On 10/30/97, OMB published "Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity" in the Federal Register. The revised standards have five categories for data on race: American Indian or Alaska Native, Asian, Black or African American, Native Hawaiian or Other Pacific Islander, and White. Additionally, there are two categories for data on ethnicity: "Hispanic or Latino" and "Not Hispanic or Latino." The FBI complies with these guidelines in its data collection programs.

79. Last October, after discussions with the FBI and others, I pointed out that the "sniper shootings" in the Washington, D.C. area could have been prevented if all states had the systems necessary to quickly transmit latent fingerprints from crime scenes to the FBI. In the sniper case, some three dozen prints from a murder-robbery in Alabama were not sent to the FBI until it was too late. I am pleased that since I identified that problem to the Bureau, five of the fifteen states that did not have the necessary connections to the FBI, including Alabama, have joined the system. However, there are still ten states where these connections do not exist. What can you do to bring these states into the system, not only to protect their own citizens but also to protect those in other states who might become the victims of offenders whose prints are already in the federal databases? If you need legislation to accomplish this, please specify what your needs are.

Response:

As of the fall of 2004, 12 states lacked the IAFIS connectivity needed to process remote latent searches from their state systems: Arkansas, Louisiana, Delaware, Vermont, Indiana, Missouri, Nebraska, New Mexico, Oregon, Nevada, Utah, and Wyoming. (In Louisiana, Oregon, and Nevada, a few local agencies can submit

to IAFIS; Indiana, Missouri, and Nebraska are in the process of establishing the needed IAFIS connectivity.) The FBI has successfully assisted many states in overcoming the hurdles of securing IAFIS latent print functionality. The FBI currently provides latent print workstation software and latent print mailer software to state and local law enforcement agencies free of charge. In return, these agencies are responsible for obtaining the workstations, scanners, printers, and compression software necessary to capture, store, and transmit latent fingerprint searches to the FBI's IAFIS. Although many non-participating states continue to show a sustained interest in pursuing IAFIS latent print functionality, obstacles encountered within these agencies have slowed their progress.

Agencies have expressed concern over the lack of funding at the state and local levels to support the purchase, installation, and operation of latent print equipment. A source of funding could help to offset costs incurred for the implementation, operation, and maintenance of latent print programs in the non-participating states. Costs include those associated with the purchase of the equipment identified above and technical maintenance contracts, as well as the costs of additional personnel, including trained operators. Additional resources would also assist participating states in further enhancing their existing operations.

Networking requirements often serve as another obstacle for agencies attempting to secure IAFIS latent print functionality. The FBI has established high speed telecommunications infrastructures between primary state locations and IAFIS; however, state and local latent print operations frequently reside in multiple locations. Therefore, these locations must employ their own networks to support the electronic routing of latent print transactions to the FBI-provided central connection. Many states have experienced problems in providing this service to users.

The FBI has developed and implemented alternate connectivity solutions to assist agencies in overcoming these challenges. Laboratories and law enforcement agencies can connect directly to the FBI by using an FBI-provided modem and encrypted dial-up service or through crime laboratory connections. To further enhance access to regional, state, and national latent print search resources, the FBI is currently developing a connectivity option that will provide access through LEO, which offers a virtual private network permitting users to securely access information through an Internet Service Provider. This service would increase the access of latent print examiners by establishing connectivity through widely available internet connections. Even with these low-cost connectivity options, agencies would still incur costs to purchase the platform and to operate and maintain the workstations.

The FBI will continue to promote the latent print functionality of IAFIS to the law enforcement community; focusing these efforts on educating the remaining states as to the importance and benefits of this service.

Questions Posed by Senator Feinstein

80. The authority to arrest and detain a person whose "testimony . . . is material in a criminal proceeding" is set forth at 18 U.S.C. 1444, "Release or detention of a material witness." The following questions pertain to the use of that provision in counterterrorism investigations and prosecutions during the period of time from September 11, 2001 to the present.

a. In how many cases have the authorities of 18 U.S.C. 1444 been used?

b. How many individuals are currently detained under the authority of 18 U.S.C. 1444?

c. In how many cases where the authority of 18 U.S.C. 1444 has been used has the individual arrested and detained in fact testified in "a criminal proceeding."

d. 18 U.S.C. 1444 prohibits the detention of any individual where "testimony of such witness can adequately be secured by deposition." In how many cases where the authority of 18 U.S.C. 1444 has been used has a deposition been taken and the witness released?

e. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 1444 has the witness been subsequently charged with a crime?

f. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 1444 has the witness be[en] subsequently transferred to the custody of the Department of Defense? Please describe the facts and circumstances of each such case.

g. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 1444 has the witness be[en] subsequently transferred to the custody of a foreign government? Please describe the facts and circumstances of each such case.

Response to questions a-g:

The correct U.S. Code citation for "Release or Detention of a Material Witness" is 18 U.S.C. § 3144. We have consistently taken the view that any details about material witness warrants are grand jury material and cannot be disclosed. Therefore, we cannot address subparts a-g of question 80.

h. What procedures and safeguards are in place to ensure that the authorities of 18 U.S.C. 1444 are not being used for purposes of preventive detention, or to hold individuals suspected of criminal activity without charging them with the commission of a crime?

Response:

Detaining an individual on a material witness warrant under 18 U.S.C. 3144 requires a showing of probable cause that: 1) the testimony of the individual is material to a federal criminal proceeding; and 2) it is impractical to secure the individual's presence by lesser means. The judicial officer issuing the warrant must be satisfied by the facts and circumstances set forth in a sworn affidavit that these criteria are met. An individual detained pursuant to a material witness warrant has the right to contest the basis for detention before the court and has the right to the assistance of an attorney. This judicial oversight and opportunity to contest the basis for detention provide safeguards against misuse of the material witness process.

I. What written policies or directives of the Department of Justice or the Federal Bureau of Investigation govern the application of the authorities set forth in 18 U.S.C. 1444?

Response:

The FBI has no internal written policies or directives governing the application for material witness warrants because an FBI Agent's role in this process is limited. While an FBI Agent may be an affiant in an application for a material witness warrant, and will work closely with a prosecutor in the drafting of the affidavit supporting the application for a material witness warrant, the application itself is drafted and submitted by a federal prosecutor.

81. In briefs filed with the Supreme Court in the matter of Padilla v. Rumsfeld, as well as in related cases and in public statements, the President and the Attorney General have asserted that the President, in his capacity as Commander-in-Chief may detain individuals, including United States citizens, as "enemy combatants." The following questions pertain to the exercise of this authority during the period from September 11, 2001 to present.

a. What role has the Federal Bureau of Investigation played in the arrest, detention, and interrogation of individuals held in custody pursuant to this authority as "enemy combatants?"

Response:

In general, the FBI does not play a role in the arrest or detention of persons designated as enemy combatants, since this is within the purview of DOD's role in the global war on terrorism. Padilla was arrested by FBI Agents in Chicago and detained in federal custody as a material witness. While in federal custody, he was designated an enemy combatant and custody was transferred to the U.S. military.

The FBI has interviewed Padilla and other enemy combatants. FBI Agents conducting interviews of enemy combatants adhere to the FBI policy governing interviews of persons in the U.S., with the one exception that enemy combatants are not advised of Miranda rights prior to the interrogation.

b. How many individuals have been arrested or detained pursuant to this authority?

c. How many United States citizens have been arrested or detained pursuant to this authority?

d. How many United States persons, as defined in Executive Order 12333, Section 3.4(I), and excepting United States citizens, have been arrested or detained pursuant to this authority?

Response to b through d:

Information concerning the designation and detention of enemy combatants is not maintained by the FBI. The Department of Defense, which is responsible for the custody and control of enemy combatants, would be the appropriate source for this information.

e. What rules, procedures or practices govern the conditions of confinement and the methods of interrogation used in cases where an individual has been arrested or detained pursuant to this authority?

Response:

Rules, procedures, and practices concerning the conditions of confinement and methods of interrogation of enemy combatants by DOD are not maintained by the FBI. When FBI Agents interview enemy combatants or detainees, standard FBI

interview policies and practices apply. The Department of Defense, which is responsible for the custody and control of enemy combatants, would be the appropriate source for this information.

82. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107-56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?

<u>Response</u>:

The FBI does not collect this information. However, we understand the Department has queried various U.S. Attorneys' Offices for this information and will forward it under separate cover as soon as it is compiled.

83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. In how many cases . . . have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?

Response:

The FBI applied for Title 18 wiretap orders in eight investigations into international terrorism since passage of the USA PATRIOT Act. In only one of those investigations was a newly added terrorism offense used as the sole predicate; traditional criminal offenses were used as the predicates for the remaining seven. It cannot be determined, however, whether probable cause as to one or more of the new terrorism predicate offenses was also established, but simply not listed, in those seven cases.

b. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates?

Response:

In the one case referred to above, the terrorism predicate was the only one asserted. It is not known, however, whether there was probable cause to believe the subjects were engaging in other predicate offenses which were simply not listed, or whether there was probable cause only with respect to the terrorism offense.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Sections 201 or 202 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?

Response:

Sections 201 and 202 of the USA PATRIOT Act are currently scheduled to expire at the end of 2005. The FBI strongly supports making these important statutory provisions permanent. In addition, the FBI would ask Congress to consider amending 18 U.S.C. 2516 to allow for the use of existing electronic surveillance authorities in investigating the full-range of terrorism related crimes. In particular, Congress should consider adding the following predicate offenses to those currently listed in 18 U.S.C. 2516(1): 1) 18 U.S.C. 37 (relating to violence at international airports); 2) 18 U.S.C. 930(c) (relating to an attack on a federal facility with a firearm); 3) 18 U.S.C. 956 (conspiracy to harm persons or property overseas); 4) 18 U.S.C. 1993 (relating to mass transportation systems); 5) an offense involved in or related to domestic or international terrorism as defined in 18 U.S.C. 2331; 6) an offense listed in 18 U.S.C. 2332b(g)(5)(B); and 7) 18 U.S.C. 2332d.

While the few statistics listed in response to questions 83 a and b, above, may be understood to indicate limited use of this new authority and limited value of these new USA PATRIOT Act sections, this would not be correct. In most international terrorism investigations since October 2001, electronic surveillance has been successfully pursued under FISA authority and, therefore, the criminal terrorism predicates under Title 18 were not necessary. Nevertheless, in future investigations in which probable cause regarding connection to a foreign power cannot be as easily established (and thus FISA surveillance is not an option), these new USA PATRIOT Act provisions will permit the use of a federal wiretap in response to significant terrorist threats. The flexibility to use either foreign intelligence collection tools or criminal evidence gathering processes, and to share the results, is an important feature of the USA PATRIOT Act in the war against terrorism.

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same [A]ct makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. Section 203© of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure of information" as provided for in Section 203.

Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response:

On 9/23/02, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the USA PATRIOT Act. Those guidelines, and the FBI's instructions to the field with respect to those guidelines, follow.

Office of the Attorney General
Washington, D. C. 20530

September 23, 2002

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM THE ATTORNEY GENERAL

SUBJECT Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons.

The prevention of terrorist activity is the overriding priority of the Department of Justice and improved information sharing among federal agencies is a critical component of our overall strategy to protect the security of America and the safety of her people.

Section 203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 278-81, authorizes the sharing of foreign intelligence, counterintelligence, and foreign intelligence information obtained through grand jury proceedings and electronic, wire, and oral interception, with relevant Federal officials to assist in the performance of their duties. This authorization greatly enhances the capacity of law enforcement to share information and coordinate activities with other federal officials in our common effort to prevent and disrupt terrorist activities.

At the same time, the law places special restrictions on the handling of intelligence information concerning United States persons ("U.S. person information"). Executive Order 12333, 46 FR 59941 (Dec. 8, 1981) ("EO 12333"), for example, restricts the type of U.S. person information that agencies within the intelligence community may collect, and requires that the collection, retention, and dissemination of such information must conform with procedures established by the head of the agency concerned and approved by the Attorney General. Section 203(c) of the USA PATRIOT Act, likewise, directs the Attorney General to establish procedures for the disclosure of grand jury and electronic, wire, and oral interception information "that identifies a United States person, as that term is defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)."

Pursuant to section 203(c), this memorandum specifies the procedures for labeling information that identifies U.S. persons. Information identifying U.S. persons disseminated pursuant to section 203 must be marked to identify that it contains such identifying information prior to disclosure.

Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801) provides:

> "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Information should be marked as containing U.S. person information if the information identifies any U.S. person. The U.S. person need not be the target or subject of the grand jury investigation or electronic, wire, and oral surveillance; the U.S. person need only be mentioned in the information to be disclosed. However, the U.S. person must be "identified." That is, the grand jury or electronic, wire, and oral interception information must discuss or refer to the U.S person by name (or nickname or alias), rather than merely including potentially identifying information such as an address or telephone number that requires additional investigation to associate with a particular person.

Determining whether grand jury or electronic, wire, and oral interception information identifies a U.S. person may not always be easy. Grand jury and electronic, wire, and oral interception information standing alone will usually not establish unequivocally that an identified individual or entity is a U.S. person. In most instances, it will be necessary to use the context and circumstances of the information pertaining to the individual in question to determine whether the individual is a U.S. person. If the person is known to be located in the U.S., or if the location is unknown, he or she should be treated as a U.S. person unless the individual is identified as an alien who has not been admitted for permanent residence or circumstances give rise to the reasonable belief that the individual is not a U.S. person. Similarly, if the individual identified is known or believed to be located outside the U.S., he or she should be treated as a non-U.S. person unless the individual is identified as a U.S. person or circumstances give rise to the reasonable belief that the individual is a U.S. person.

Grand jury and electronic, wire, and oral interception information disclosed under section 203 should be received in the recipient agency by an individual who is designated to be a point of contact for such information for that agency. Grand jury and electronic, wire, and oral interception information identifying U.S. persons is subject to section 2.3 of EO 12333 and the procedures of each intelligence agency implementing EO 12333, each of which place important limitations on the types of U.S. person information that may be retained and disseminated by the United States intelligence community. These provisions require that information identifying a U.S. person be deleted from intelligence information except in limited circumstances. An intelligence agency that, pursuant to section 203, receives from the Department of Justice (or

another Federal law enforcement agency) information acquired by electronic, wire, and oral interception techniques should handle such information in accordance with its own procedures implementing EO 12333 that are applicable to information acquired by the agency through such techniques.

In addition, the Justice Department will disclose grand jury and electronic, wire, and oral interception information subject to use restrictions necessary to comply with notice and record keeping requirements and as necessary to protect sensitive law enforcement sources and ongoing criminal investigations. When imposed, use restrictions shall be no more restrictive than necessary to accomplish the desired effect.

These procedures are intended to be simple and minimally burdensome so that information sharing will not be unnecessarily impeded. Nevertheless, where warranted by exigent or unusual circumstances, the procedures may be modified in particular cases by memorandum of the Attorney General, Deputy Attorney General, or their designees, with notification to the Director of Central Intelligence or his designee. These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

The guidelines in this memorandum shall be effective immediately

Precedence: PRIORITY **Date:** 11/05/2002

To: All Divisions **Attn:** Assistant Directors
Deputy Assistant
Directors
Section Chiefs
SACs
ASACs
Chief Division Counsels
JTTF Supervisors

From: Office of the General Counsel
Front Office, Room 7159
Contact: Charles M. Steele, (202) 324-8089
Elaine N. Lammert, (202) 324-5640

Approved By: Gebhardt Bruce J
Ashley Grant D
D'Amuro Pasquale J
Wainstein Kenneth L
Steele Charles M

Drafted By: Steele Charles M:cms

Case ID #: 62F-HQ-C1382989

Title: GUIDANCE ON NEW ATTORNEY GENERAL GUIDELINES ON SHARING FOREIGN INTELLIGENCE INFORMATION ACQUIRED IN CRIMINAL INVESTIGATIONS AND RELATED GUIDELINES

Synopsis: This EC provides guidance on the new Attorney General Guidelines on sharing foreign intelligence information acquired in the course of criminal investigations.

Details: On 9/23/02 the Attorney General issued three new sets of guidelines implementing sections 905 and 203 of the USA PATRIOT Act. Copies of the guidelines are enclosed; they are

also posted on the Office of the General Counsel's (OGC) website, in the Law Library webpage.[2] All employees should become familiar with the guidelines and with the guidance set forth in this EC.

1. Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of A Criminal Investigation

From an operational standpoint, these are the most important of the new guidelines. They will significantly affect the way in which the FBI approaches criminal investigations. The guidelines implement the mandate of section 905(a) of the PATRIOT Act that federal law enforcement agencies "shall expeditiously disclose to the Director of Central Intelligence [DCI], pursuant to guidelines developed by the Attorney General in consultation with the Director, foreign intelligence acquired ... in the course of a criminal investigation."[3] This is an affirmative statutory duty: the FBI (and other federal law enforcement agencies) must share foreign intelligence information (as defined in the guidelines) acquired in criminal investigations. The new guidelines are intended to institutionalize, formalize, and enhance such information sharing, which has been going on since passage of the PATRIOT Act, in order to further the FBI's primary mission of detecting and preventing acts of terrorism.

---

[2] On 9/24/02, the new guidelines were announced and posted on the FBI Intranet homepage. On 9/25/02, OGC notified all Chief Division Counsels (CDCs) by e-mail of the issuance of the guidelines. On 10/8/02, OGC notified all HQ Divisions by e-mail of the issuance of the guidelines, and directed them to the OGC webpage.

[3] The guidelines also require that foreign intelligence information be disclosed to designated Homeland Security officials. No such officials have yet been designated for purposes of receiving foreign intelligence. OGC will provide notification when such designations are made.

The procedures established by the guidelines for the sharing of foreign intelligence information with intelligence agencies are not intended to replace or supersede existing operational or information sharing mechanisms (e.g., information sharing that goes on in the context of Joint Terrorism Task Forces (JTTFs)). Agents should continue to use such mechanisms, subject to the guidelines.

The disclosure obligation extends to grand jury and Title III information which contains foreign intelligence information. Section 203 of the PATRIOT Act permits disclosure of such information to the CIA, notwithstanding prior legal impediments (e.g. the grand jury secrecy rule). Section 905(a), however, goes further, and requires that all such information be expeditiously disclosed.

"Foreign intelligence," as used in the guidelines, is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." This definition comes from the National Security Act of 1947, 50 U.S.C. § 401a.

Some of the more important provisions of the guidelines are summarized below.

Training (Guidelines ¶ 3)

The guidelines, and Section 908 of the PATRIOT Act, require the Department of Justice (DOJ) (in consultation with the DCI and other officials) to develop a training curriculum and program to ensure that law enforcement officials receive sufficient training to identify foreign intelligence subject to the disclosure requirement. Training is critical to the successful implementation of the guidelines; it is crucial that law enforcement agents be able to recognize foreign intelligence information subject to the disclosure requirement. In some

instances it will be obvious that certain information constitutes foreign intelligence information; in other cases it may not be so clear.

DOJ and the FBI are consulting with the CIA to formulate and implement a training curriculum and program, which will include training for both new and onboard Agents. CIA personnel will participate, providing instruction on how to identify the types of foreign intelligence information needed by the Intelligence Community.

Further details will be provided when the training curriculum is finalized.

Entities to Whom Disclosure Shall be Made (Guidelines, ¶ 4)

The guidelines require the DCI, in consultation with the Assistant to the President for Homeland Security, to designate appropriate offices, entities and/or officials of intelligence agencies and homeland security offices to receive the disclosure of section 905(a) information not covered by an established operational or information sharing mechanism. The DCI is to ensure that sufficient numbers of recipients are identified to facilitate expeditious sharing and handling of section 905(a) information. The DCI has not yet identified recipients pursuant to this provision; OGC will provide notification when recipients are designated.

Note that these designated recipients will come into play only where there isn't already "an established operational or information sharing mechanism." Guidelines, paragraph 4. Where there are already established mechanisms (e.g. JTTFs), FBI Agents can and should use them to disclose 905(a) information.

Methods for Disclosure of Section 905(a) Information

To: All Divisions From: Office of the General Counsel
Re: 62F-HQ-C1382989, 11/05/2002

(Guidelines, ¶ 5)

The guidelines divide foreign intelligence information into two categories: (1) information relating to terrorism or weapons of mass destruction (WMD),[4] and (2) all other types of foreign intelligence information. Similarly, the guidelines address two different categories of terrorism/WMD information: that which relates to "a potential ... threat," and "other" terrorism/WMD information.

Foreign intelligence information relating to a "potential terrorism or WMD threat to the United States homeland, its critical infrastructure, key resources (whether physical or electronic), or to United States persons or interests worldwide" must be disclosed "immediately." Guidelines, ¶ 5(a). All other foreign intelligence information (including all other foreign intelligence information relating to terrorism or WMD information, e.g. information relating to the financing of a terrorist organization, or to an organization's long-term recruitment plans) must be disclosed "as expeditiously as possible."[5]

Whether particular terrorism/WMD foreign intelligence information relates to a "potential threat" (i.e. requiring immediate disclosure) will depend on the facts and circumstances of the particular situation. Clearly, information indicating the planning or commission of an imminent act of terrorism will fall into this category. On the other hand, foreign intelligence information relating to long-term recruiting efforts by a terrorist organization will have to be disclosed

---

[4] "Terrorism information" and "weapons of mass destruction," for purposes of the guidelines, are defined in ¶ 5(a), at page 4.

[5] As to section 905(a) information other than that relating to terrorism and WMD, the guidelines require federal law enforcement agencies, in consultation with DOJ and the DCI, to develop (or continue to follow existing) protocols to provide for expeditious sharing. ¶ 5(b), at page 4.

expeditiously, but not immediately. The upcoming training will help clarify what information is so related to a "potential threat" that it must be disclosed immediately; for the time being, Agents should exercise sound judgment in making the determination, keeping in mind that the ultimate purpose for the disclosure requirement is to help "disrupt[] terrorist plans, prevent[] terrorist attacks, and preserv[e] the lives of United States persons." Guidelines, ¶ 5(a).

Disclosure may be made in the following ways: (1) through existing field-level operational or information sharing mechanisms (e.g. JTTFs); (2) through existing headquarters operational or information sharing relationships; or (3) when the law enforcement officer reasonably believes that time does not permit the use of any such established mechanisms, through any other field level or other mechanism intended to facilitate immediate action, response or other efforts to address a threat. (I.e., if an Agent reasonably believes that the circumstances require immediate action, he or she should take whatever steps are necessary to share the information with the appropriate intelligence agency immediately. This could mean, for example, picking up the phone and calling a point of contact he or she has with the CIA.)

As soon as practicable after disclosing section 905(a) information (under any of the above-referenced mechanisms), the disclosing Agent must notify the relevant JTTF (e.g., the JTTF supervisor) of the disclosure. JTTFs, in turn, must keep the relevant Anti-Terrorism Task Force (ATTF) (e.g., the United States Attorney's Office representative on the ATTF) apprised of the nature of information disclosed under the guidelines. JTTFs are not required to notify ATTFs of every disclosure of foreign intelligence information; DOJ recognizes that such a requirement would be impractical. JTTFs, however, should take steps to keep ATTFs generally apprised of the nature of section 905(a) information disclosed; JTTFs should also ensure that ATTFs are specifically advised of particularly important disclosures (e.g. disclosures relating to specific threats). Whether a particular

disclosure is important enough to warrant specific notice to the ATTF is a judgment call. ATTFs shall, in turn, apprise DOJ's Terrorism and Violent Crime Section (TVCS) of section 905(a) disclosures. (Also: where section 905(a) information is disclosed at the headquarters level, the disclosing headquarters entity shall, as soon as practicable and to the extent reasonable, notify TVCS of all disclosures.)

It has not yet been decided whether a single, standard procedure will be developed to govern how JTTFs will notify ATTFs, or rather whether each JTTF will be asked to develop its own mechanism. That matter is under consideration at FBIHQ. In the meantime, each JTTF should preliminarily develop its own mechanism for notifying ATTFs, taking into account its own particular structure, personnel, existing communication channels with ATTFs, etc.

Consultation With Prosecutors With Respect to Title III and Grand Jury Information (Guidelines, ¶ 5(c))

In order to avoid harm to pending or anticipated prosecutions, the guidelines establish requirements for pre-disclosure consultation with prosecutors in certain situations. Specifically, the guidelines state that, except as to terrorism/WMD information related to a potential threat, the law enforcement agent must consult with the prosecutor assigned to the case if (1) the information was developed through investigation occurring after a formal referral for prosecution, and (2) the information was produced by a Title III interception or solely as a result of a grand jury subpoena or testimony occurring before a grand jury receiving information concerning the particular investigation.

This consultation requirement serves the important purpose of allowing the prosecutor to decide whether to impose use restrictions (as set forth in ¶ 8 of the guidelines) or to

seek an exception to the disclosure requirement (as set forth in ¶ 9 of the guidelines).

This pre-disclosure consultation with the prosecutor must be accomplished expeditiously. An Agent who consults with a prosecutor pursuant to this provision should document the fact of the consultation, including the date and time of the contact with the prosecutor. If the prosecutor concurs with disclosure, the Agent must make the disclosure no later than 48 hours after the prosecutor is initially notified. If the prosecutor objects, the Agent should obtain and document the prosecutor's reasons and, if the Agent disagrees with the prosecutor's position, consult with his or her supervisors. (The Agent should not disclose the information, however, until the disagreement with the prosecutor is fully resolved.) If the Agent does not have a decision from the prosecutor as of 48 hours after the initial contact, the Agent should contact the prosecutor to determine the prosecutor's position.

Title III or grand jury-generated section 905(a) information which an Agent reasonably believes is related to a potential terrorism or WMD threat shall be disclosed immediately, without need for advance consultation with the prosecutor. Contemporaneously or as soon after making such disclosures as possible, the Agent shall notify the prosecutor (to enable the prosecutor to make any required notice to the court).

Requests for Additional Information (Guidelines, ¶ 6)

Initial disclosure of section 905(a) information shall be accomplished automatically, without specific prior request to the disclosing agency. Requests by any recipient for additional information, or for clarification or amplification of the initial disclosure, should be coordinated through the component that provided the initial information or the designated HQ office of the disclosing agency.

To: All Divisions From: Office of the General Counsel
Re: 62F-HQ-C1382989, 11/05/2002

Disclosure of Grand Jury and Title III Information (Guidelines, ¶ 7)

Where grand jury or Title III information is shared under the guidelines, notice of such disclosures must be promptly provided to DOJ's Office of Enforcement Operations (OEO).[6] Agents do not have to contact OEO themselves; that is the obligation of the AUSA or DOJ prosecutor assigned to the grand jury matter or Title III.

The PATRIOT Act also requires special procedures for the disclosure of grand jury and Title III information that identifies United States persons. Those procedures are set forth in the second set of guidelines issued on 9/23/02 and discussed below. Also, all of the procedures established pursuant to those guidelines are made applicable to all disclosures under these guidelines of section 905(a) information that identifies United States persons.

Use Restrictions (Guidelines, ¶ 8)

Generally, the guidelines contemplate that 905(a) information will be disclosed without imposition of use restrictions. However, the disclosing official may impose appropriate use restrictions necessary to protect sensitive law enforcement sources and pending criminal investigations and prosecutions.

The scope and duration of any such restrictions must be tailored to address the particular situation. Any such restrictions must be no more restrictive than necessary to accomplish the desired effect. Also, the originator of the information must periodically review the restrictions to

[6] The guidelines require OEO to establish appropriate record keeping procedures to ensure compliance with notice requirements related to the disclosure of grand jury information. Guidelines, ¶ 7.

determine whether they can be narrowed or lifted at the request of the recipient.

Finally, disclosures of grand jury and Title III information must be subject to any use restrictions necessary to comply with record or notice keeping requirements, and to protect sensitive law enforcement sources and pending criminal investigations and prosecutions. Agents should consult with the AUSA or DOJ prosecutor assigned to the grand jury matter or Title III to determine what use restrictions, if any, are necessary in each case.

AG Exceptions to Mandatory Disclosure (Guidelines, ¶ 9)

Section 905(a) authorizes the Attorney General, in consultation with the DCI, to exempt from the disclosure requirement one or more classes of foreign intelligence or foreign intelligence relating to one or more targets or matters. Paragraph 9 of the guidelines implements this provision. It states that pending the development of permanent exceptions, exemptions will be determined by the Attorney General, in consultation with the DCI and the Assistant to the President for Homeland Security, on a case-by-case basis.

No permanent exceptions have yet been developed. OGC will provide notification if and when permanent exceptions are developed.

Requests for exceptions must be submitted "by the department, component or agency head in writing with a complete description of the facts and circumstances giving rise to the need for an exception and why lesser measures such as use restrictions are not adequate." Guidelines, ¶ 9(c). Authority to request exceptions has not yet been delegated below the level of component agency head (and it is not clear whether it will

be). For now, therefore, FBI requests for exceptions can only be submitted by the Director.

Any FBI requests for exceptions should be submitted for review and approval to CID and CTD. CID and/or CTD will then forward the requests to the Director's Office. OGC will be available to provide assistance with regard to any such requests.

Closed Investigations

OGC has concluded, in consultation with DOJ, that there is no legal impediment to sharing foreign intelligence information acquired in criminal investigations which have been closed. Field offices should therefore identify closed criminal investigations which appear likely to have developed foreign intelligence information; if any such information is found, it must be disclosed pursuant to the guidelines.

Field offices need not conduct comprehensive general searches of all closed files, or of broad categories of closed files. If, however, there is reason to believe it is likely that particular closed files contain foreign intelligence information, the field office should conduct reviews of those files.

2. Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons

Section 203 of the PATRIOT Act authorizes the sharing of foreign intelligence, counterintelligence, and foreign intelligence information obtained through grand jury proceedings

and Title III interceptions with relevant Federal officials[7] to assist in the performance of their duties. At the same time, section 203(c) requires the Attorney General to establish procedures for the disclosure of grand jury and Title III information that identifies United States persons.[8]

These new guidelines implement section 203(c) by establishing the required procedures for labeling grand jury and Title III information which identifies United States persons. Such information must be marked, prior to disclosure, to indicate that it contains such identifying information. Information should be marked if it identifies <u>any</u> United States person (i.e. the person need not be a target or a subject). However, the United States person must be "identified;" i.e., the grand jury or Title III information must discuss or refer to the U.S. person by name (or nickname or alias), rather than merely including potentially identifying information (e.g. an address or telephone number) which requires additional investigation to link to a particular person.

For the time being, no particular language or method of marking is required.[9] The information must be clearly marked, however, in a manner which will ensure that the recipient will immediately understand that the information identifies United States persons. One way to do this, for example, would be to place the information in a sealed envelope marked with the following language in conspicuous lettering:

---

[7]The information may be shared with any Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials receiving that information in the performance of his official duties. Fed. R. Crim. P. 6(e)(3)(C)(V) (grand jury information); 18 U.S.C. § 2517(6) (Title III information).

[8]"United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section. 50 U.S.C. § 1801.

[9]FBIHQ is considering whether to institute a single, standard method of marking.

To: All Divisions From: Office of the General Counsel
Re: 62F-HQ-C1382989, 11/05/2002

"NOTE: THIS PACKAGE CONTAINS INFORMATION WHICH IDENTIFIES UNITED STATES PERSON(S)." Agents should also specifically direct the recipient to the references to identified U.S. persons.

Agents need not rely solely on the grand jury or Title III information itself in determining whether the information identifies a United States person; Agents may also use the context and circumstances of the information in making that determination.

If the person is known to be located in the U.S. (or if his or her location is unknown), he or she should be treated as a U.S. person unless circumstances give rise to the reasonable belief that he or she is not a United States person. Similarly, if the person is known or believed to be located outside the U.S., he or she should be treated as a non-United States person unless he or she is identified as, or circumstances give rise to the reasonable belief that he or she is, a United States person.

Receiving agencies are to designate individuals as points of contact for purposes of receiving this information. (No such designations have yet been made; OGC will provide notification when designations are made.) Also, receiving agencies are to handle such information in accordance with their own procedures implementing Executive Order 12333 (which governs such agencies' collection and use of such information).

3. Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources

These guidelines implement section 905(b) of the PATRIOT Act, which requires the Attorney General to develop guidelines to ensure that DOJ responds within a reasonable period of time to reports from the intelligence community of

possible criminal activity involving foreign intelligence sources or potential foreign intelligence sources.

Section 905(b) and the guidelines reflect a recognition that in such situations the referring intelligence community agency may have a strong interest in knowing on an expedited basis whether DOJ intends to investigate potential crimes.

Accordingly, the guidelines require DOJ to confer expeditiously (and not later than seven days after the referral) with the referring intelligence community agency. After conferring, DOJ shall inform the referring agency within a reasonable period of time (not more than 30 days, except in extraordinary circumstances) whether it intends to commence or decline a criminal investigation.

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

This communication should be distributed to all employees within your division. In particular, please ensure prompt distribution to all Special Agents and other appropriate investigative personnel.

♦♦

CC: 1 - Mr. Bruce Gebhardt
1 - Mr. Grant Ashley
1 - Mr. Pasquale D'Amuro
1 - Mr. Kenneth Wainstein
1 - Mr. Charles Steele
1 - Mr. M.E. Bowman

To: All Divisions From: Office of the General Counsel
Re: 62F-HQ-C1382989, 11/05/2002

1 - Mr. Patrick Kelley
1 - Ms. Elaine Lammert
1 - Mr. James Lovelace
1 - Mr. John Livingston

b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any means appropriate to the circumstances, including Intelligence Information Reports (IIRs), Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(b) material?

Response:

The FBI disseminates intelligence information via the IIR, which is an electronic communication format widely accepted in the IC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence (intelligence which has not been finally evaluated) and associated clarifying information that puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers. Before FBI intelligence is disseminated, it is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities that may be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify intelligence that is consistent with IC intelligence requirements and interests.

(1) If so, how many such reports have been issued?

Response:

Although CTD is not the only FBI producer of IIRs, that Division reports that, during the period from August 2002 (when statistical data was first collected) through August 2004, CTD has disseminated approximately 3,860 IIRs, 240 of which have contained FISA-derived intelligence. The remaining IIRs have been

derived from various sources and methods which may or may not include Title III information.

The FBI does not track or maintain a central database with respect to the number of IIRs containing 203(b) material, if any.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Determinations to disseminate electronic, wire, and oral intercept information are made with input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when appropriate, DOJ. This evaluation considers the value of the information not only to the IC but also, depending on the proposed use, context, and nature of any threat-related information, to federal, state, and local law enforcement entities and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies.

The quality and value of IIRs are evaluated through several means. On each IIR, the Reports Officer provides information by which the customers can contact the Reports Officer directly. The quality and relevance of the reporting is also reflected by the submission of additional collection requirements; IC members often forward formal Requests for Information (RFIs) with respect to information that has been protected (not provided) in the IIR, such as U.S. Person information. Such RFIs provide an excellent indication of IC interest in FBI reporting. In addition, IC members often provide feedback with respect to specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. The FBI's OI also often receives evaluations of FBI reporting, and is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response:

The FBI shares foreign intelligence information, as defined in Section 203(d)(2), with the IC through several conduits. Dissemination can be through direct classified and unclassified IIRs, Intelligence Assessments, Intelligence Bulletins,

Teletype Memoranda, or IC web sites on classified networks. The FBI also shares intelligence information through the FBI's Joint Terrorism Task Forces (JTTFs), which include members of the IC and operate in 100 locations across the United States. Unclassified but "law enforcement sensitive" intelligence information is also disseminated to federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments and trends.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any appropriate means, including IIRs, Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(1) If so, how many such reports have been issued?

Response:

While the FBI does not track or maintain a central database with respect to the number of IIRs containing 203(d) material, if any, the July 2004 DOJ "Report From the Field: The USA PATRIOT Act at Work" indicates that DOJ has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, to track terrorists' funding sources, and to identify terrorist operatives overseas.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

There are various means by which IIRs are evaluated. Members of the IC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify the means by which customers can contact them directly. IC members assess the quality and relevance of the reporting, and submit additional collection requirements when appropriate. Often, IC members forward formal Requests for Information (RFIs), which can provide an excellent indication of IC interest in FBI reporting. The FBI's OI also receives evaluations of FBI reporting. The OI is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

d. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response:

Pursuant to Section 905, DOJ developed the Attorney General's Guidelines Regarding Information Sharing under the USA PATRIOT Act. These guidelines are available on the website of DOJ's Office of Legal Policy (OLP) (www.usdoj.gov/olp). Additionally, among other Department materials relating to information sharing are the following:

- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Part VII.B. (10/31/03) (concerned in part with information sharing with intelligence agencies) – Portions of these guidelines are classified, but Part VII.B., relating to information sharing, is unclassified and appears without deletions on OLP's website.

- Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (3/4/03).

- Memorandum from the Attorney General entitled, "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation" (9/23/02) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Coordination of Information Relating to Terrorism" (4/11/02) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Prevention of Acts Threatening Public Safety and National Security" (11/8/01) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Disseminating Information to Enhance Public Safety and National Security" (Sept. 21, 2001) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

e. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

f. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

Sections 203(b) and (d) should not be allowed to expire on 12/31/05, since the changes afforded by the USA PATRIOT Act have significantly increased the ability of the FBI to share information.

85. Section[ ] 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains [to] the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. How often has this authority been used, and with what success?

Response:

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

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response:

FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. The FBI shares many forms of foreign intelligence with other members of the IC through direct classified and unclassified disseminations, through web sites on classified IC networks, through its participation in Joint Terrorism Task Forces (JTTFs), and through its collaboration in activities abroad.

FBI intelligence products shared with the IC include IIRs, Intelligence Assessments, and Intelligence Bulletins. The FBI also disseminates intelligence information through LEO, a virtual private network that reaches federal, state, and local law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes available to all users finished FBI intelligence products, including intelligence assessments resulting from the analysis of criminal, cyber, and terrorism intelligence, finished intelligence concerning significant developments or trends, and IIRs that are available at the SBU level. In addition, the FBI recently posted the requirements document on LEO, providing to state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response:

In the past two years, CTD's Terrorism Reports and Requirements Section has disseminated 76 IIRS containing information derived from FISA-authorized surveillance and/or searches. (Statistics are not maintained in a way that would enable us to advise whether any of the FISA-derived information in the reports was obtained using roving wiretap authority.) Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 IIRs containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

The OI promulgated the FBI's Intelligence Information Report Handbook on 7/9/04. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The OI is also working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with law enforcement and IC partners.

In addition, the FBI's Inspection Division has established criteria for assessing: the value of human source reporting; access to and the responsiveness of local FBI field offices; and FBI program and national intelligence requirements. The OI is developing guidelines for using these same criteria to assess the value of raw intelligence. Initial discussions on this issue have been held with the CI, CT, Criminal, and Cyber Divisions, and the results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response:

No, DOJ does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept

the conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, for surveillance of all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the FISA Court issue, along with the primary order, a "generic" secondary order with respect to a specifically identified FISA target that the FBI can serve in the future on a currently unknown cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear, in a detailed affidavit, to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. While the roving order carries the additional requirement of a judge's approval to monitor more than one telephone, it permits government agents to continue to monitor the target, even if the target changes to a different cellular telephone, rather than first going through the lengthy application process to monitor that new phone. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the FISA Court for a new secondary order. The FBI views this as a vital tool to follow targets who change cell phone providers or other communication channels as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response:

The FBI does not file briefs with the FISA Court. While OIPR files briefs with that Court on behalf of DOJ and the government, it has filed no such briefs on this subject.

d. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

Response:

We are not aware of any systematic reviews in this area, either by the FBI or DOJ.

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?

Response:

None of which the FBI is aware.

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

None at this time.

87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since passage of this act?

Response:

The FBI does not collect or maintain statistics concerning the types of search warrants issued in FBI investigations, including those seeking access to voice mail. Because federal search warrants are requested by U.S. Attorneys' Offices and issued by U.S. District Courts, these statistics may be maintained by one or both of those offices.

b. In such cases, have there been any instances in which a wiretap, as opposed to a search[ ] warrant[,] would not have been supported by the facts asserted in support of the search warrant.

Response:

This information is unavailable, as indicated above. It is clear, however, that the support needed for a federal wiretap is considerably greater than that required for a search warrant.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

A private citizen who has lodged numerous complaints against the FBI, all of which have been determined to be unfounded pursuant to appropriate inquiry, complained that she was a former FBI employee whose home, vehicles, telephone, and internet had been subject to "aggressive surveillance" since August 2000. FBI investigation revealed that the complainant was, in fact, not a former FBI employee and that the FBI had conducted no surveillance of her for any reason. Based on these findings, this matter was closed by the FBI in July 2003. The FBI has construed this as a complaint with respect to both Section 209 and 217 of the USA PATRIOT Act.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI is not aware of any substantive changes to this provision warranting Congressional consideration. Section 209 is, however, currently scheduled to expire at the end of 2005, and the FBI strongly supports making this provision permanent. Section 209 allows investigators to use court-ordered search warrants to obtain voice-mail messages held by a third party provider when supported by probable cause. Previously, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. 2703, allowed law enforcement authorities to use search warrants to gain access to stored electronic communications such as e-mail, but not stored wire communications such as voice-mail. Instead, the wiretap statute, 18 U.S.C. 2110(1), governed access to stored wire communications, requiring law enforcement officers to use wiretap orders to gain access to unopened voice-mail. This resulted in voice-mail messages being treated differently than e-mail messages. Voice-mail messages are also treated differently than answering machine messages inside a home, access to which requires a search warrant, because answering machine messages are not regulated under the wiretap statute. Section 209 of the USA PATRIOT Act eliminates the disparate treatment of similar information. If this section is sunsetted, voice-mail messages will again be treated in a different manner than answering machine messages and stored e-mail information beginning in 2006.

88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.

a. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.

Response:

Service providers have voluntarily provided information on at least 141 occasions under this provision. Such disclosures have often included both e-mail content and associated records. Several of these disclosures have directly supported terrorism cases under the emergency of a possible pending attack. For example, this provision has been used to obtain access to e-mail accounts used by terrorist groups to discuss various terrorist attacks. It has also been used to respond quickly to bomb and death threats, as well as in an investigation into a threat to a high ranking foreign official. This provision has additionally been used to locate kidnaping victims and to protect children in child exploitation cases. In one kidnaping case involving the abduction of a 14-year-old girl, reliance on this

provision allowed the FBI to quickly locate and rescue the child and to identify and arrest the perpetrator. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours.

Because many international service providers are located within the United States (such as Hotmail and AOL), Legal Attachés have used this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss of life or serious injury.

Additional examples are provided in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work."

b. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant, would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.

Response:

We are aware of no such circumstances. However, it is important to recognize that the information that may be disclosed under this emergency authority is limited to the contents of communications that are in electronic storage and records associated with customers or subscribers. Given this limitation, a conventional wiretap would generally not apply, and a search warrant would be required only for the contents of communications in 'electronic storage' (e.g., incoming email not yet retrieved by the subscriber) less than 181 days old. Emergency authority is appropriate for the disclosure of information held by a third party and, to the extent the information is constitutionally protected, disclosure of the information under exigent circumstances is entirely consistent with the emergency exception to the warrant requirement of the Fourth Amendment.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

There is currently a discrepancy between the emergency provisions applicable to contents and records that appears illogical and unjustified. Currently a provider is arguably required under 18 U.S.C. 2702(c)(4) to meet a higher burden for disclosing a record or other subscriber information than is required by § 2702(b)(7) for divulging the contents of a communication in electronic storage. Moreover, the entities to whom a provider may disclose are significantly more restricted for records than for content. The language in (b)(7) was enacted by Pub. L. 107-296 as part of the Homeland Security Act of 2002, with the objective that all entities with responsibility for ensuring our domestic security would have access to this information in an emergency. It does not appear that the discrepancies between the disclosure of content and records are supported by differing privacy interests inherent in the respective information or by other factors. Accordingly, reconciling these provisions would be appropriate.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

Response to a and a(i):

The FBI does not maintain this information. It is, instead, maintained by DOJ's OIPR, to whom the FBI defers for response.

b. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response:

The FBI does not track the number of pen registers that evolve into full FISA's.

c. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

Response:

The FBI has not developed any such regulations or directives, nor is it aware that the IC or DOJ have issued guidance defining "non-content communications" in relation to the use of FISA pen register/trap and trace authorities.

d. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

See response to Question 85b, above.

(i) If so, how many such reports have been issued?

Response:

See response to Question 85b(i), above.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

See response to Question 85b(ii), above.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be conducted solely on the basis of activities protected by the First Amendment.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA). At the FBI field level, such requests must be approved by the Supervisory Special Agent (SSA), the SAC or appropriate Assistant SAC, and the Chief Division Counsel. At the FBIHQ level, the request must be approved by an attorney in the National Security Law Branch, and signed by one of the several designated high-ranking FBI officials to whom certification authority has been delegated. Thereafter, the request is submitted to DOJ's OIPR, and must be approved by OIPR before it is presented to the FISA Court. When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The only instance when the Department has declassified the number of times section 215 has been used was on 9/18/03 – not in October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated 12/23/04.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, however, terrorists and spies have used libraries to plan and carry out activities that threaten our national security, and it is important that we not permit these facilities to become safe havens for terrorist or other illegal activities. The PATRIOT Act permits those conducting national security investigations to obtain business records – whether from a library or any other business – with the permission of a federal judge.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence

activities conducted by the IC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

None of the information contained in the 3,860 terrorism-related IIRs disseminated between August 2002 and August 2004 was acquired pursuant to section 215 of the USA PATRIOT Act.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information acquired pursuant to section 215 of the USA PATRIOT Act.

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.

a. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.

Response:

While the FBI does not maintain statistics on the frequency with which the trespasser authority has been used, we can provide examples of some such cases.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). This group used chat rooms and fraudulent web sites, creating false identities to obtain e-mail accounts and then transmitting their communications through a computer that had been "hacked" and set up to operate as their proxy server. A proxy server changes an Internet user's original Internet protocol (IP) address to that of the proxy server so that only the proxy server knows the true point of origin. The owner of the hacked computer was not aware that it was being used as a proxy server, and considered all individuals using the system as a proxy server to be trespassers. The owner provided the FBI with consent to monitor the communication ports solely used by the trespassers, and this monitoring led to the subject's true identity. The subject was indicted in September 2003. Without this authority to monitor, the real identities of the trespassers could easily have remained anonymous.

In another example, a former employee was suspected of illegally accessing a company's e-mail system to gain inside information regarding company concepts and client information, as well as privileged information regarding legal proceedings between the company and the former employee. The computer intruder used a variety of means to access the system, including wireless modems in laptops and hand-held Blackberry devices, making it more difficult to identify the intruder and to link the computer intrusions to the former employee. The victim company authorized the FBI to monitor the intruder's communications with and through its computer systems.

In another case, a computer-intruder obtained control of a school's network and reconfigured it to establish additional IP addresses that were separate and distinct from those used by the school. This allowed hackers, and others using the Internet who did not want to be located, to jump through the school's system before committing their illegal acts. Monitoring accomplished pursuant to the school's consent resulted in the FBI's identification of over 200,000 different IP addresses using the school system as a proxy to further illegal activity such as fraud, computer intrusions, and spamming.

As these cases make clear, this authority is critical not only to the FBI's ability to identify criminals who engage in computer intrusions but also its ability to

identify and investigate additional criminal activities conducted through victims' computers.

b. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?

Response:

Yes. As with any form of consent, which must be freely and voluntarily given to be valid, the consenting party has the right to terminate the consent at any time. The FBI encourages the use of a written consent form containing an express acknowledgment by the consenting owner or operator that states: "I understand my right to refuse authorization for interception and have accordingly given this authorization freely and voluntarily."

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

See response to Question 87c, above.

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

Response:

As indicated in the July 2004 DOJ publication entitled, "Report from the Field: The USA PATRIOT Act at Work," the removal of the "wall" played a crucial role in the Department's successful dismantling of a Portland, Oregon, terror cell, popularly known as the "Portland Seven." Members of this terror cell had

attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned through an undercover informant that, before the plan to go to Afghanistan was formulated, at least one member of the cell, Jeffrey Battle, had contemplated attacking Jewish schools or synagogues, and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they suspected that a number of others were involved in the Afghanistan conspiracy. While several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them. Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack; if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would undoubtedly have scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets, and could keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely, but instead to continue to gather evidence on the other cell members. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on 10/3/03.

DOJ shared information pursuant to sections 218 and 504 before indicting Sami al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist organizations, responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that al-Arian served as the secretary of the PIJ's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ. Sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to prosecutors' ability to build their case and pursue the proper charges.

Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, some of whom trained for jihad in Northern Virginia by participating in paintball and paramilitary training or traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against several individuals. Nine of these defendants have received sentences ranging from four years to life imprisonment (six of these sentences were pursuant to guilty pleas and three were contrary to their pleas; charges have included conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban).

Information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was also pivotal in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. Based upon information obtained through an FBI undercover investigation, the complaint alleges that Al-Moayad had boasted that he had personally handed Usama Bin Laden $20 million from his terrorist fund-raising network and that Al-Moayad and Zayed had flown from Yemen to Frankfurt, Germany, in 2003 with the intent to obtain $2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

Sections 218 and 504 were also used to gain access to intelligence that facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden, and used his charities both to obtain funds for terrorist organizations from unsuspecting Americans and to serve as a channel for people to contribute money knowingly to such groups. Arnaout pled guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the San Diego prosecution of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they had conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they had conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

Sections 218 and 504 were also critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq and of two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA shared information with law enforcement agents and prosecutors investigating Dumeisi. Through this coordination, law enforcement agents and prosecutors learned from intelligence officers that an April 2003 telephone conversation between Dumeisi and a co-conspirator corroborated evidence that Dumeisi was acting as an agent of the Iraqi government, providing a compelling piece of evidence at Dumeisi's trial.

b. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA

PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FISA Court of Review has made clear that the "significant purpose" standard is constitutional. Accordingly, additional changes are unnecessary.

93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.

a. In how many cases has this authority been used?

Response:

While the FBI does not require or maintain centralized statistics on the use of search warrants, Field Offices indicate that they have routinely relied on this provision (codified at 18 U.S.C. 2703(a)) and can safely estimate that, nationwide, this search authority has been used at least 100 times since its passage.

In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The ability to obtain this information with greater efficiency has proven invaluable in numerous cases, including: several terrorism investigations (such as the Virginia Jihad case described above and a complex terrorism financing case in which it was used to obtain a subject's e-mail related to a 7/4/02 shooting at Los Angeles International Airport); child pornography cases in which it is used to obtain information from ISPs regarding those trading sexually exploitive images of children; investigations of "carders" (those who use and trade stolen credit card information); and numerous investigations into Internet sales of counterfeit products, which have led to several indictments and the seizure of bank and financial accounts.

Child pornography cases highlight the benefit of Section 220, because the ability to obtain a search warrant in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the ISP is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country so they could obtain warrants in those jurisdictions, or travel hundreds or thousands of miles to present warrant applications to local magistrate judges. Without Section 220, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

The following case, included in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work," provides an additional example of the benefits afforded by Section 220. A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he contacted cooperating individuals by e- mail using an Internet service provider (ISP) located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, including the California ISP. Within a day of the order's issuance, the ISP released information revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Because they were aware that the fugitive had previously worked as a carnival worker, the Deputy Marshals went to the carnival and discovered the stolen car, arresting the fugitive as he approached the car. He later pled guilty in state court and was sentenced to imprisonment for 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to his capture.

Section 220 has also made the process of obtaining a warrant for ISP information much more efficient. Before the USA PATRIOT Act, judicial districts that are home to large ISPs were inundated with search warrant requests for electronic evidence. For example, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for the records of an ISP located there. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all the details of another district's investigation in order to present an affidavit to the court in support of the search warrant application. Because of section 220, however, these attorneys and Agents can now spend their time on local cases and investigations rather than on learning the details of unrelated investigations being worked

through distant offices. Given the short time for which ISPs typically retain records, this provision has enabled the FBI to obtain critical information that may otherwise have been lost or destroyed in the ordinary course of the ISP's business. Section 220 also results in a more efficient use of judicial resources by allowing the judge with jurisdiction over the offense to issue the warrant and retain oversight over the search.

b. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

94. Section 223 of the USA-Patriot Act creates a cause of action for willful violations of Title III's electronic surveillance procedures. Have any such lawsuits been brought? If so, please provide details of each such case.

Response:

No such lawsuits have been brought.

95. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked? If so, please describe any such case.

Response:

No. Immunity has not been claimed under this section with respect to FBI investigations in either the civil or criminal context.

96. The following question pertains to surveillance conducted pursuant to the FISA.

a. What is the backlog on processing of intercepts? What is the average time between interception and first monitoring.

b. What percentage of intercepts that are not in English are translated within 24 hours? A week?

c. How many hours of FISA intercepts remain untranslated as of May 20, 2004?

Response to a through c:

FBI Director Mueller has made clear his interest in having all material derived from the FBI's use of FISA authority reviewed and analyzed as quickly as possible. Since the majority of this material is in languages other than English, FBI Language Services Section personnel meet with the FBI's National FISA Manager and other management officials every two weeks to discuss national operational priorities and the most effective utilization of finite linguist resources. The operational plan established by this meeting is modified almost daily based on ever-shifting investigative priorities. These tactics ensure that all of the highest priority intelligence collected in a foreign language is reviewed immediately and that any outstanding work is limited to matters assigned a lower relative priority.

The FBI currently has sufficient translation capacity to promptly address all translation needs with respect to its highest priority, CT operations, often within 12 hours. While there are instances in which the FBI is not able to address translation needs as quickly as it would like, such as when the language or dialect involved is initially unidentifiable, this usually pertains to lower priority matters.

Conventional digital systems used to collect FISA-derived materials were not designed to measure the average time between intercept and initial monitoring. Recognizing the tactical value of having such aging reports for command and control purposes, a nationally integrated FISA statistical collection and reporting system has been developed and is undergoing a test and evaluation process to validate the mapping of meta data. This system should be fully functional by the end of calendar year 2004. It is clear, however, based on information provided by FBI field office managers, that the vast majority of communications in a foreign language relating to terrorism operations are being afforded full review by a qualified linguist within, at most, a few days of collection.

d. Please describe the process of indexing and retrieving FISA material.

Response:

Intelligence summaries from FISA intercepts are indexed and archived according to strict electronic surveillance (ELSUR) rules that make these summaries part of the official FBI record and allow these records to be searched in the Field Offices where the cases reside. Although recent progress has been made in creating an electronic archive of CI material that can be searched by authorized users fieldwide, CT summaries from FISA audio intercepts are not searchable in a central database at this time. The phased deployment of the ELSUR Data Management System (EDMS), starting in FY 2005, will make all intelligence summaries from FISA intercepts available in a searchable archive.

e. In the past 5 years, has there been a review or audit of the accuracy of FBI translations of intercepted or seized foreign language material?

Response:

Historically, translation reviews were normally conducted by field office managers on a semi-annual basis in conjunction with a linguist's performance appraisal rating. In order to standardize this procedure, the FBI's Language Services Section implemented minimum quality control standards and guidelines and assumed central management of the language services quality control program in January 2003. Quality control program guidelines stipulate which linguists' translations must be reviewed and at what intervals. The guidelines also identify those materials that must always be reviewed prior to dissemination.

Questions Posed by Senator Feingold

FBI Role in Iraq

97. a. How many special agents, translators, and other FBI employees have been assigned to work in Iraq since March 2003 and how many are currently there?

Response:

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

b. Where were these agents, translators, and other employees assigned before they were sent to Iraq?

Response:

They were assigned to many of the FBI's offices, both in the field and at FBIHQ.

c. How many of these agents, translators, and other employees were working in the United States on terrorism cases?

Response:

15 percent of the FBI employees sent to Iraq were working on terrorism cases prior to that deployment.

FBI DNA Lab

98. The U.S. Department of Justice and Jacqueline Blake, a former biologist at the FBI DNA laboratory, recently entered into a plea agreement. Blake pled guilty to authoring and submitting over 100 reports containing false statements regarding DNA analysis she performed during a 2-1/2 year period from 1999 to 2002.

a. According to a Justice Department press release, the FBI has retested evidence in many of Blake's cases and has concluded that her false statements did not affect the outcome of any of the criminal cases in which she was involved. I assume that the FBI has notified the prosecutors in those cases. Has the FBI notified the courts and defense attorneys in each case in which Blake's falsified reports were involved? If not, why not?

Response:

In April 2002, DNA Analysis Unit I (DNAU I) discovered that one of its biological laboratory technicians, Jacqueline Blake, had systematically and repeatedly violated the Unit's standard operating procedure (SOP) by failing to process to completion mandatory negative control samples within the Short Tandem Repeat (STR) process. Ms. Blake worked under the direction of a qualified DNA examiner, who relied upon the data generated by Ms. Blake for the development and issuance of the corresponding reports of examination. Promptly following this discovery, the FBI reported the violation to the DOJ OIG through the FBI's Office of Professional Responsibility (OPR).

The DNAU I determined that Ms. Blake had inaccurately represented that negative control samples had been utilized properly, and had been involved in the processing of 103 case submissions. OIG attorneys obtained an affidavit from Ms. Blake, in which she acknowledged willful misconduct. Ms. Blake subsequently pled guilty to falsifying documentation on which DNAU I examiners relied for interpretation and reporting purposes.

Since the discovery of Ms. Blake's misconduct, the FBI Laboratory has made it a priority to notify those law enforcement entities and prosecutors affected by Blake's misconduct. Because these entities represent the entry point of any laboratory results into the criminal justice system, the FBI believes this notification will ensure that Blake's actions, and the FBI Laboratory's response to these actions, are properly disseminated. In addition to prosecution and law enforcement officials, all agencies that received DNA reports in which Ms. Blake performed STR processing were also notified of Blake's failure to complete testing of the negative control samples, rendering the written report unsuitable for investigation or prosecution purposes. This notification included telephonic, mail, and facsimile contact. In the majority of these cases, no judicial action had occurred and no prosecutor had been assigned, largely because most of the reported cases did not have subjects identified for comparison. Where prosecutors had been assigned, they were notified and clearly informed of their disclosure obligations.

b. As you know, after complaints and calls for reform in the 1990s and after a Justice Department Inspector General report in 1997 concluded that the lab's scientists engaged in bad science and gave inaccurate testimony, the FBI conducted an extensive overhaul of its DNA lab, which included implementing a peer review system to prevent the exact kind of situation that has occurred here. Please describe that peer review system and explain how and why it failed in this case.

Response:

While the 1997 OIG report did not address the FBI's DNA analysis, a May 2004 OIG report does address this issue. Since the establishment of DNAU I in 1988, it has routinely applied two forms of review on every case, including a technical review to ensure the completeness and accuracy of the interpretive data and conclusions and an administrative review to check for overall content and adherence to unit reporting policies. Ms. Blake's misconduct went undetected primarily because her willful falsification of case file documentation deceived the technical review process and enabled her to conceal her misconduct. As indicated below, the FBI Laboratory is implementing procedural changes to prevent such deception in the future.

c. As a result of the peer review system's failure in this case, what is the FBI doing to revise its system to prevent this kind of breakdown from happening again?

Response:

As previously indicated, the technical or peer review process did not fail, but rather was compromised by Ms. Blake's falsification of documents. Upon discovery of this misconduct, the DNAU I immediately expanded the scope of its peer review process to specifically address Ms. Blake's breach of integrity. The peer review process now requires documentation demonstrating verification of the complete processing of all negative control samples, and this documentation is verified by the examiner of record, the peer reviewer, and the administrative reviewer. Additionally, the DNAU I is implementing procedural changes to further augment its quality practices, consistent with the OIG's May 2004 recommendations regarding the protocols and practices of the FBI's nuclear DNA laboratory.

d. I understand that the Inspector General has been pushing the FBI to conduct regular audits of state and local labs that place DNA evidence into the national DNA registry. What steps are you taking to improve oversight of state and local labs to ensure that labs placing information in the national registry are placing accurate information?

Response:

The FBI Laboratory's interim plan for review of the accuracy, completeness, and acceptability of DNA profiles in the National DNA Index System (NDIS) will consist of having FBI auditors evaluate the classification, accuracy, and

completeness of the DNA profiles when performing case file reviews during Quality Assurance audits. The Audit document has been revised to include a reminder that FBI auditors must conduct this review, and a form has been prepared to record review results. Additional guidance for NDIS participants and auditors on the standards for including DNA profiles in NDIS is contained in the CODIS Administrator's Handbook. The FBI is also creating positions for CODIS auditors, who will develop a permanent plan for the review of DNA profiles uploaded to NDIS. These positions have been approved and the hiring process has begun.

U.S.S. Cole Bombing Investigation

99. In October 2000, the U.S.S. Cole was attacked during its stop in the harbor of Aden, Yemen, resulting in the deaths of 17 crew members, including one of my constituents, and wounding 39 others. On April 11, 2003, 10 men, including men suspected of involvement in the Cole bombing, escaped from a prison in Yemen. I understand that the suspects have now been recaptured.

a. What steps did the FBI take to determine how the suspects escaped? Has the FBI determined who facilitated their escape?

Response:

Although an FBI Legal Attaché reported to Sana'a in March 2004, there was no FBI Legal Attaché assigned in Yemen at the time of the April 2003 escape. Therefore, the FBI obtained information related to this escape from the U.S. Embassy in Sana'a and other members of the IC.

Additional information with respect to this question is classified and is, therefore, provided separately.

b. What steps have been taken by the FBI to evaluate the security of the detention facility in which these suspects are currently being held?

Response:

The defendants in the U.S.S. Cole trial are being held in a secure facility in Sana'a, Yemen, rather than in the Aden facility from which Al-Badawi and Al-Quso escaped. While the FBI team in Sana'a is working closely with Yemeni authorities with respect to this trial, we are not in a position to assess the security

of this detention facility. Information related to the security of Yemeni detention facilities is better addressed by the U.S. Embassy in Sana'a.

c. Has the FBI interviewed the suspects since they have been recaptured?

Response:

Upon the re-capture of Al-Badawi and Al-Quso, the FBI requested authority to interview them, particularly with respect to the April 2003 escape. These suspects were then in the custody of the Yemen Political Security Organization (PSO), which ultimately authorized these interviews. By that time, however, Al-Badawi and Al-Quso had been transferred from the PSO's custody to that of the Prosecutor General's Office for prosecution. The trial of Al-Badawi, Al-Quso, and other U.S.S. Cole defendants began on 7/7/04 in Sana'a, Yemen.

d. What is the status of the FBI's investigation of these suspects and the Justice Department's plans to pursue a prosecution?

Response:

The FBI's investigation into the attack on the U.S.S. Cole is ongoing. In May 2003, Al-Badawi and Al-Quso were indicted by a Federal Grand Jury in the Southern District of New York for their roles in the Cole attack. In April 2004, the FBI requested the renditions of Al-Badawi and Al-Quso via diplomatic note. The Yemen Ministry of Foreign Affairs (MFA) responded that "the rendition request must be supported by legal documents in order to look into the matter according to Yemeni Law." Based on this reply, the Southern District of New York was asked for the necessary documents (such as the U.S.S. Cole indictment and arrest warrants for Al-Quso and Al-Badawi) so they can be provided to the MFA.

Timika, Indonesia Investigation

100. a. Please provide an update on the status of the FBI investigation into the murder of American citizens in Timika, Indonesia, on August 31, 2002.

Response:

The FBI developed sufficient evidence to obtain an indictment in U.S. Federal Court on 6/16/04. The subject charged with the 8/31/02 murders is Anthonius

Wamang, a member of the military branch of the Free Papua Movement, commonly known as OPM.

b. Has the FBI been able to conduct all the interviews it desires to conduct without the presence of Indonesian military minders undermining the integrity of the interview? Has the FBI obtained access to all the evidence to which it wants access? Is the FBI encountering any obstructions to the investigation at all?

Response:

The FBI is satisfied with the current level of cooperation from the Indonesian military (TNI). Recent cooperation by the TNI reflects a commitment to allowing the FBI direct access to some of their most sensitive human sources in a way that will permit effective interviews by FBI Agents.

c. What are the ramifications for the FBI's investigation of statements made by Indonesian military officers who have commented to the press about what the FBI has concluded about TNI involvement?

Response:

These comments by TNI officers, as well as unofficial statements by U.S. officials, dramatically affect the level of cooperation offered by those who perceive themselves as subjects of the investigation. These leaks also negatively affect the security of FBI investigators and individuals cooperating with the FBI.

Brandon Mayfield Fingerprint Identification and Detention

101. On May 24th, a federal court dismissed the material witness proceeding against Brandon Mayfield, an attorney and former U.S. Army officer. In written submissions to the court and in public statements the FBI has admitted that the fingerprint of Mayfield was mistakenly matched to a fingerprint recovered at the scene of the May 11, 2004, Madrid train bombing.

a. When were Mayfield's fingerprints taken and when and why were they entered and maintained in the Integrated Automated Fingerprint Identification System (IAFIS)? If Mayfield's fingerprints were maintained in the IAFIS system because of his prior military service, what percentage of former members of the military currently have their fingerprints in IAFIS?

b. The FBI has stated that members of the Latent Print Unit (LPU) went to Madrid on two occasions to discuss the accuracy of the Mayfield fingerprint identification.

(I) What were the dates of the two trips to Madrid?

(ii) In addition to members of the LPU, who from the FBI or DOJ also traveled to Madrid on each of the trips?

(iii) During the first trip to Madrid, what specific information did the Spanish National Police provide to the FBI and DOJ about the accuracy and reliability of the Mayfield fingerprint identification?

(iv) As a result of the first trip to Madrid, what if any efforts were taken to confirm that Mayfield's fingerprints had been correctly identified?

c. The FBI has stated that an international panel of fingerprint experts will review the LPU examination in the Madrid bombing.

(I) Will the Spanish National Police be involved in this review?

(ii) What will be the scope of the review of the international panel?

(iii) Will the international panel be allowed to review the process leading up to the inclusion of Mayfield's fingerprints in the IAFIS system?

(iv) Will the results of the international review be made available to Congress?

d. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

e. Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.

Response to a through e:

As indicated above, the FBI will defer response during the pendency of the OIG and OPR reviews and the Mayfield lawsuit.

Use of the USA PATRIOT Act

102. In October 2003, the Department reported that as of April 1, 2003, it had sought, and courts had ordered, delayed notice warrants 47 times.

a. As of the date of your response to these questions, or some reasonable recent date, how many times has the Department sought and received authorization to execute a delayed notification search since enactment of the PATRIOT Act?

Response:

The FBI does not collect this information. However, we understand the Department has queried various U.S. Attorneys' Offices for this information and will forward it under separate cover as soon as it is compiled.

b. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "seriously jeopardized an investigation"? For each such delayed notice warrant, please describe how granting contemporaneous notice would have seriously jeopardized the investigation and please indicate whether seriously jeopardizing the investigation was the sole basis or one of multiple grounds for delaying notice.

c. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "unduly delayed a trial"? For each such delayed notice warrant, please describe how requiring contemporaneous notice would have unduly delayed a trial and please indicate whether unduly delaying a trial was the sole basis or one of multiple grounds for delaying notice.

Response to b and c:

This information was not collected in the EOUSA survey and is not otherwise available except through individual U.S. Attorney's Offices. Nevertheless, because these questions focus on the sufficiency of the grounds offered to justify a delay, it should be noted that a district court judge or magistrate must find "reasonable cause" to believe the grounds forwarded in the affidavit exist and are

sufficient to justify the delay. In addition, notice is only delayed; it is never eliminated. The searched party will, therefore, have the opportunity to challenge the validity and sufficiency of the reasons for delay and, if those reasons prove to be insufficient, to seek an appropriate remedy.

d. How many of the delayed notice warrants were issued with a (I) seven-day or less delay; (ii) 8 to 30 day delay; (iii) 31 to 60 day delay; and (iv) time period of 61 days or more and what were those time periods?

e. How many of the delayed notification warrants issued since the PATRIOT Act was passed were used in non-terrorism criminal matters?

f. Please provide the case name, docket number, and court of jurisdiction for each case in which a delayed notice warrant was issued since enactment of the PATRIOT Act.

Response to d through f:

This information was not collected in the EOUSA survey and is not otherwise available except through individual U.S. Attorney's Offices.

103. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

104. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

Response:

The requirements of the SAFE Act are inconsistent with, and more restrictive than, the requirements applicable to roving wiretaps in criminal investigations. In criminal cases, roving wiretap orders are limited to "such time as it is reasonable to presume that the [target] is or was reasonably proximate" to the facility. 18 U.S.C. 2518(11)(b)(iv). This does not require a conclusive determination that the target is actually present at the time of interception, as the SAFE Act would require, but only a reasonable belief under the circumstances that the facility or place is being used by the target. An analogous requirement is already contained in the Foreign Intelligence Surveillance Act (FISA). Under FISA, the FBI must demonstrate probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. 1805(a)(3)(B). In addition to these safeguards, both Title III and FISA require the use of procedures

to minimize the acquisition, retention, and dissemination of information concerning innocent persons.

As a practical matter, the standard required by the SAFE Act would preclude most, if not all, roving wiretaps under FISA. Frequently, it is impossible or impractical to ascertain a target's presence through physical observation. A limited review of the context and substance of intercepted communications may be the only means of confirming the target's presence, particularly when multiple, similar-sounding individuals are using the same device. This is especially true when the intercepted communications are in a foreign language. Under the SAFE Act, electronic surveillance could not be used to ascertain the presence of the target. Thus, roving FISA wiretaps would be limited to those circumstances in which the target's presence could be confirmed by physical observation.

b. The SAFE Act would also require the FBI to identify either the target of the wiretap or the place to be wiretapped. For example, in the event that the FBI has a physical description of the target but does not know the identity of the target, the SAFE Act would allow the FBI to conduct a "John Doe" wiretap by identifying the facilities to be wiretapped. This is a sensible requirement to protect innocent Americans who are not the target of an investigation, while still allowing the FBI to conduct surveillance of suspected terrorists or spies. Why shouldn't Congress enact this prudent safeguard? Please explain.

Response:

A "roving" wiretap is one linked to a particular investigative target, regardless of the facility being used by that individual. The purpose of the "roving" authority is to allow uninterrupted, court-ordered monitoring of the target, even when the target changes facilities to thwart surveillance. Thus, by definition, the facility or place at which a "roving" surveillance is directed cannot be known at the time the order is issued. The SAFE Act would preclude this type of uninterrupted surveillance of investigative targets who successfully conceal their identities.

Under current law, a FISA wiretap application must include "the identity, if known, or a description of the target of the electronic surveillance." 50 U.S.C. 1805(c)(1)(A). The SAFE Act would eliminate roving wiretaps in cases where the FBI is able to provide a description of the target, but has been unable to determine the target's identity.

The SAFE Act's limitation of the roving authority under FISA appears unwarranted because, even in cases where the target's identity is unknown, the FBI must still describe the individual target with sufficient specificity to demonstrate probable cause to believe "the target of the electronic surveillance is

a foreign power or an agent of a foreign power." 50 U.S.C. 1805(a)(3)(A). This probable cause requirement, which must be read together with the "description" requirement of 50 U.S.C. 1805(c)(1)(A), protects innocent Americans who are not the targets of investigations.

Questions Posed by Senator Durbin

105. You testified that terrorism prevention is the top priority of the Bureau and that resources have been diverted within the Bureau in support of this important effort. However, the fight against terrorism should not come at the cost of diminished law enforcement in critical areas such as criminal civil rights violations. Please discuss what resources if any have been diverted away from the FBI's Civil Rights Program since September 11, 2001.

Response:

Immediately after 9/11/01, there was an increase in the FBI resources dedicated to address the surge in backlash hate crimes committed against Arab, Muslim, and Sikh Americans. Once these backlash hate crimes became less frequent, the resources dedicated exclusively to the investigation of civil rights matters decreased to the pre-9/11 level. In spite of this decrease in civil rights resources, the FBI's response in addressing civil rights matters has not diminished. The CRP is among the FBI's top 10 priorities, and appropriate resources have been allocated to it. When an office's resources available to address civil rights matters are strained, the SAC of that field office has the authority to pull resources from other, lower-priority programs to address civil rights matters. This has allowed the FBI to remain vigilant and focused on assigning appropriate resources to address violations of federal civil rights statutes when they occur.

106. I commend the FBI for its effectiveness in investigating troublesome increases in hate crimes and human trafficking. After September 11, our nation witnessed a disturbing increase in hate crimes committed against individuals in the United States who appear to be of Muslim, Middle Eastern, and South Asian descent, and the FBI has effectively investigated this spike in hate crimes and provided valuable assistance to prosecutors. Similarly, the Department of Justice has vigorously prosecuted human trafficking cases, and the FBI has played an important role in investigating these barbaric crimes. However, the FBI is also the lead investigative component within the Department of Justice involving other important criminal civil rights violations, such as police misconduct and the Freedom of Access to Clinic Entrances (FACE) Act. Has the focus on hate crime and trafficking investigations resulted in a reduction of investigations in other critical areas of civil rights enforcement? Please explain.

Response:

The investigative resources the FBI devotes to address backlash hate crimes targeting the Arab, Muslim, and Sikh communities, and to the increasing focus on human trafficking matters, have not resulted in a diminished focus on the other subprograms within the CRP.

In articulating the FBI's top priorities after the tragic events of 9/11/01, the Director designated the protection of civil rights among the FBI's top 10 priorities. As a result, as indicated in response to Question 105, above, if a Field Office's resources available to address civil rights matters are strained, the SAC has the authority to pull resources from other, lower-priority programs to ensure that civil rights matters are appropriately addressed.

107. Please indicate the number of investigations the FBI has opened each year over the past ten years regarding: (A) hate crimes, (B) human trafficking, (C) police misconduct and other "color of law" violations, (D) FACE violations, and (E) other criminal civil rights violations.

Response:

The chart below reflects the number of Hate Crime, Involuntary Servitude/Slavery (ISS), Color of Law (COL), and FACE Act cases opened by the FBI since 1994. The chart does not contain a category for "other criminal civil rights violations" because these four subprograms capture all civil rights cases investigated by the FBI.

FY	Hate Crimes	ISS	COL	FACE	TOTAL
1994	1604	13	3063	0	4680
1995	736	28	2638	45	3447
1996	855	3	2582	227	3667
1997	919	9	2729	97	3754
1998	878	14	2799	84	3775
1999	801	18	2411	91	3321
2000	729	51	2276	59	3115
2001	751	54	1797	42	2644
2002	652	58	1385	23	2118
2003	478	65	1345	20	1908
(End 2nd Qtr) 2004	167	26	614	9	816

108. According to the FBI's website, there are two units within the Civil Rights Program that investigate criminal civil rights violations: the Color of Law Unit and the Hate Crimes Unit. Your website indicates that the Hate Crimes Unit has investigatory authority over not only hate crimes but also human trafficking and FACE violations.

a. Is your website accurate in this regard? If not, please explain the current organizational scheme for the investigation of criminal civil rights violations.

Response:

No. In June 2002, the Hate Crimes Unit and the Color of Law Unit were combined to form the CRU. The FBI is currently in the process of updating the website to reflect this change in organizational structure.

b. Has the Hate Crimes Unit received an increase in the number of agents over the past three years? Please provide data about the number of agents who have served in the Hate Crimes Unit each year over the past ten years. Please provide similar data about the number of agents who have served in the Color of Law Unit each year over the past ten years. Please indicate whether any other FBI agents are assigned to the Civil Rights Program.

Response:

The number of Supervisory Special Agents (SSAs) in the former Hate Crimes Unit and Color of Law Unit, now combined to form the CRU, has remained relatively constant over the past ten years. The CRU, which has program and case management responsibilities, has a funded staffing level of six and is currently staffed with five SSAs.

Perhaps more helpful to an understanding of the FBI's commitment to civil rights investigations is the FBI's FSL of 153 Agents in the CRP. The chart below reflects the CRP's FSL and "work years" since 1997, the earliest year for which these numbers are available. The work years include all CRP work done, whether by Agents assigned to the CRP or to other programs. These work years exceed the FSL in years in which Agents outside the CRP worked on civil rights cases, but they are less than the FSL when Agents assigned to the CRP are required to work on other matters, such as on CT or CI investigations.

FY	Work Years	FSL
1997	182.12	156
1998	155.41	156
1999	189.55	155
2000	161.63	153
2001	141.38	153
2002	104.47	153
2003	114.16	153
(End 2nd Qtr) 2004	120.32	153

109. Some people have expressed concern that there may not be a sufficient number of agents working in the Bureau's Civil Rights Program to meet the challenges of increased numbers of hate crime and human trafficking violations, in addition to police misconduct and FACE.

a. Do you believe that the FBI has a sufficient number of agents in its Civil Rights Program, or do you believe that more agents are needed? If the latter, how many more agents are needed?

Response:

Currently, the CRP's FSL is 153 Agents. Because only a few field offices are using more Agent work-hours for the CRP than they are allotted, it does not appear that an increase in the number of Agents assigned to the program is necessary. However, ISS cases have increased substantially over the last several years due to improved community awareness of these matters. If this trend continues, additional Agents may be needed. A future terrorist attack could also cause an increase in backlash hate crimes against those believed to be of the same ethnicity as the terrorists, which could require additional civil rights investigative resources. Finally, while the level of resources needed to address FACE Act crimes should remain relatively static, a single, high profile, violent act could reverse this trend and necessitate the dedication of additional program resources.

b. What efforts if any have you undertaken to request more agents for the Civil Rights Program? Please discuss specific recommendations you have made, if any, to obtain additional personnel for this program.

c. If you have requested more agents for the Civil Rights Program, have you been successful in obtaining them? If so, please indicate how many additional agents you have received. If not, please explain whether your requests were denied by Congress, by personnel within the Department of Justice, or by personnel within the White House or Office of Management and Budget.

Response to b and c:

The FBI works with DOJ and the Administration to determine its budget requirements. It is the Administration's policy that pre-decisional information concerning the level of these requirements not be released. In FY 2002 through 2005, no additional Civil Rights personnel were included in the budget request to Congress. However, in FY 2004 Congress added nine support positions to the FBI's Civil Rights complement.

110. According to the FBI's website, the two units within the Civil Rights Program "provide training to FBI New Agents, Field Agents, National Academy Attendees and other state/local police officers from around the country." Please describe all training that the Civil Rights Program has provided over the past three years regarding enforcement of human trafficking, hate crimes, FACE, and police misconduct laws for (A) new FBI agents, (B) FBI agents who serve in the Bureau's investigative programs other than the Civil Rights Program, (C) state and local police officers, indicating the departments in which those officers serve, and (D) other National Academy Attendees, indicating the law enforcement units in which those attendees serve.

Response:

As previously discussed in response to Question 108a, above, the FBI's website contains outdated information regarding the existence of two units responsible for civil rights violations, rather than reflecting that those two units have been combined to create the CRU. The CRU provides civil rights training to all FBI New Agents' classes, covering the four subprograms within the CRP. Since FY 2002, the CRU has conducted 56 two-hour blocks of New Agent instruction.

With few exceptions, Agents who serve in other FBI investigative programs do not receive training in civil rights matters aside from the initial training received as a New Agent trainee. One exception occurs when an Agent is temporarily assigned to the CRP, in which case the Agent would receive civil rights training.

Civil Rights training for state and local law enforcement agencies is provided regularly by the FBI Field Offices. A roster specifically identifying the agencies

that have received training from the FBI would be voluminous; over the past three years more than 180 agencies have received FBI training in more than 330 civil rights training sessions. CRU personnel also periodically conduct civil rights training for state and local law enforcement officials based upon requests from FBI field offices, United States Attorneys' Offices, and DOJ.

In addition, the CRU conducts quarterly training sessions for the FBI's NA attendees. A roster specifically identifying these agencies would be voluminous; approximately 1,000 NA attendees receive this training annually.

111. Some FBI agents who have served in the Civil Rights Program have stated that this investigative program is not considered a prestigious program within the Bureau or a stepping stone to leadership within the Bureau.

a. What is your response to this assertion?

Response:

The assertion that the CRP is not considered a stepping stone to leadership positions within the Bureau is inaccurate. The number of civil rights investigators who are ultimately promoted is comparable to the promotion rates in other programs, such as the White Collar Crime, Organized Crime, and Violent Crime/Major Offender Programs. Although CT promotional opportunities may be the greatest due to the size of that program, civil rights investigators are afforded an opportunity to gain the CT knowledge they need to be competitive for senior CT positions through readily available training and TDY opportunities.

b. What is the Bureau doing to demonstrate to its personnel that civil rights positions within the Bureau are prestigious and career-advancing posts?

Response:

The FBI demonstrates the importance of civil rights positions by acknowledging those who have contributed to and achieved within the program through promotions and awards, including Quality Step Increases and other incentive awards. In addition, a significant number of Agents assigned to civil rights matters have been nominated and have received national recognition for their investigative efforts through the highly prestigious Attorney General's Award for Excellence and the Director's Distinguished Service Award.

112. The FBI website indicates that your agency co-chairs a subcommittee of the Attorney General's Hate Crimes Working Group.

a. Is this working group still in existence? If so, please describe its duties and responsibilities, how often it meets, and please identify the members of the subcommittee and working group.

Response:

As DOJ advised in response to questions posed to Attorney General Ashcroft following his 6/8/04 hearing before the Senate Judiciary Committee, in 1997 Attorney General Janet Reno asked the Office of the Deputy Attorney General to establish a Hate Crimes working group to examine the problem of bias-motivated crimes including: legislative initiatives, data collection, community outreach, prosecution and enforcement, and coordination. The working group fulfilled its mandate in October 1997, when it submitted to the Attorney General a memorandum outlining specific proposals. These proposals were approved by the Attorney General, and formed the basis for the Department's hate crimes initiative. In December 1997, the Attorney General directed the implementation of the hate crimes initiative. The Department (including U.S. Attorneys' Offices, the Civil Rights Division, and the FBI) continues to vigorously investigate and prosecute bias-motivated crimes.

Since September 2001, federal, state, and local authorities have investigated over 600 alleged incidents of religiously or racially motivated backlash crime. State and local prosecutors have brought charges in nearly 150 of these incidents (in a number of cases, with federal assistance). In addition, federal charges have been brought in 22 cases against 27 defendants, resulting in 20 convictions and one acquittal (one defendant committed suicide prior to trial). Currently, eight defendants are awaiting trial or sentencing.

b. Has the FBI taken a position on whether it supports the bipartisan Local Law Enforcement Enhancement Act of 2003, S. 966? If so, please indicate whether you support or oppose this bill.

Response:

DOJ did not take a position with respect to this 108th Congress legislation.

ENCLOSURE

QUESTION 16
TRILOGY CONTRACT CHRONOLOGY

MEMORANDUM

TO: Contract File
GSA Contract No. GS00T99ALD0210
Task Order T0001AJM028

From: Shelly Goergen
FEDSIM Contracting Officer
and
Paul R. Thornton
FEDSIM PM/COR, FBI Trilogy UAC

Re: Trilogy User Application Component (UAC) Task Order
Historical Document - Trilogy UAC Task Order

Date: January 26, 2005

INTENT OF TRILOGY UAC HISTORICAL DOCUMENT

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

FBI VISION FOR TRILOGY UAC

TRILOGY is intended to be a three year project for upgrading the IT capabilities and associated support services throughout all of the sites for the Federal Bureau of Investigation (FBI). TRILOGY organizes the FBI IT infrastructure into three functional components: User Applications Component (UAC), Information Presentation Component (IPC), and Transportation Network Component (TNC).

The goal of the User Applications Component (UAC) is to replace the available current investigative applications and present the data via an easier user interface with enhanced functionality. To achieve improved data access the FBI envisions an improved search and indexing capability to access all relevant data subject to security and access constraints. The FBI also envisions documenting and managing investigative cases from inception to closure via an electronic "Virtual" Case File (VCF), to include multimedia. The envisioned system will result in the consolidation and simplification of processes and significantly reduce the dependence on paper transfer and filing, as well as paper forms.

The VCF goal is to capture information once, organized by outcomes, not functions, on the premise that information will be widely shared and distributed. The FBI also envisions the UAC to provide a reliable, dynamic, centrally administered Web-site. The centrally administered Web-site will provide users the ability to employ the Intranet to search and retrieve information, upload and download information including manuals, FBI documents, forms and personnel announcements. To optimize performance, and to better administer, manage, and support users, the FBI envisions consolidating all Intranet pages into a centralized infrastructure.

The Enterprise Management System (EMS) lies within the TNC, at the intersection of all TRILOGY components (the UAC, IPC, and TNC). The EMS will provide FBI IT Infrastructure management for the IPC, TNC, and UAC. The EMS will provide basic management and control of network assets and software. The EMS will provide users with an around-the-clock TRILOGY Help Desk. The TRILOGY Help Desk support shall augment the current operations.

TRILOGY UAC TIMELINE

DATE:	**February 7, 2001**
ACTION:	**RFP To Millennia Contractors**

On February 7, 2001, FEDSIM sent a notice to all Millennia Contractors regarding Task Order Request (TOR) GSC-TFMG-01-M028. This TOR provides support to the FBI to modernize the IT infrastructure across the FBI, and focuses solely on satisfying the requirements of the UAC of TRILOGY (i.e. TOR does not include IPC/TNC requirements).

The FBI established priorities for the TRILOGY UAC, based on FBI mission needs. **The original priority of the Trilogy UAC TOR was to improve technology first, then address usability.** The FBI needed to correct IT infrastructure problems, which made it difficult to use legacy investigative applications. The historical lack of an Enterprise IT strategy resulted in dozens of legacy stove-piped databases. In addition, the old system did not operate the way agents do their jobs, and there were incomplete on-line case files due to:

Lack of basic multi-media support

Low confidence/faith in the system by agents and users. They couldn't get to it, or they simply did not use it.

As a result, vendors were solicited to provide the following Technology Refreshment solutions:

Update the system hardware and software

Move the data to modernized databases

Provide a web interface

Re-host the applications

It was NOT the FBI's original intent to

Re-engineer the data and business processes

Create a single physical database

Build custom applications and software around Users' requirements

Overhaul the security and access control mechanisms

DATE:	**June 5, 2001**
ACTION:	**Trilogy UAC Task Order Award issued**

On June 5, 2001, the FBI UAC Task Order was issued to Science Applications International Company (SAIC) under the Millennia Contract (GS00T99ALD0210), as a result of TOR GSC-TFMG-01-M028 and Amendments 0001 and 0002. Services for this award were specified in SAIC's proposal dated 3-19-2001. The total estimated value of the Task Order award was $87,785,931.

CLIN Ceilings

CLIN 1 (Labor)	61,397,931.00
CLIN 2 (Long Dist. Travel)	300,000.00
CLIN 3 (ODCs)	25,000.00
CLIN 4	26,063,000.00
Total Contract Value	**87,785,931.00**

DATE:	September, 2001
ACTION:	POST 9-11
IMPACT:	PROBLEM AREAS IDENTIFIED (with current direction of Trilogy UAC Task Order)

The terrorist activities of 9-11-01 resulted in the identification of the following "problem areas" with the current direction of the existing Trilogy UAC Task Order:

Potential scale and complexity of investigations (e.g., PENTTBOM) could not be managed with original approach
Agents would have limited ability to analyze data across FBI cases and systems with the original approach (information still stovepiped) – "Don't know what we know."
Information sharing with other federal agencies, state and local law enforcement not fully addressed
Business processes needed to change – "How cases are managed."
IT organization was driving the "process," instead of Agent community needs
Technology upgrades were simply not going to address existing problems

Subsequent to September 11, 2001, the FBI identified the need to accelerate work under Task Order T0001AJM028 in support of the FBI Trilogy UAC. The UAC component of Trilogy will upgrade and enhance the five major existing (legacy) investigative software applications: Automated Case Support (ACS), Criminal Intelligence Support Program (CISP), Integrated Intelligence Information Application (IIIA), Criminal Law Enforcement Application (CLEA) and Telephone Application (TA) functionality and data. The terrorist attacks of September 11, 2001 ignited an effort to accelerate the development schedule of Trilogy, which already had an aggressive 3-year schedule. Trilogy has important impacts on all FBI locations and addresses the needs of both the agents and their support community. Trilogy is particularly important for the investigation of the September 11, 2001 terrorist attacks on the United States and the potential for further attacks, including the recent anthrax episodes. Approximately 50 percent of the FBI Field Offices, adjunct offices, headquarters, and other classified components of the FBI are involved in the terrorist attack investigation. In response to the events of September 11, the FBI Director instructed that Trilogy be deployed faster than the current contracted schedule with the deployment to be completed in July 2002. Congress recognized the importance of this schedule

acceleration and passed legislation to provide additional funding for the FBI's efforts. The FBI Director and a FBI team drove key Trilogy UAC decisions that included the following:

Stop Work on web-enabling existing applications (user interface updates would not improve effectiveness).
Recognition that adding functionality to initial UAC would be cost ineffective (marginal enhancements would be expensive and increase overall schedule risk).
FBI Agents and users must determine operational solutions via:
- Re-engineering of the case management process & data relationships (system must support the process, not the reverse)
- Re-engineering that is based on the VCF concept
- Active and continuous user involvement

Replans between September 2001 and January 2002, included:

Web Enabling Replan (Sept. '01)
ACS Acceleration Mainframe Centric Architecture Replan (Sept. '01)
- Oracle Proposal Replan (Nov. '01)
- Programmatic Alternatives Replan (Nov./Dec. '01)
- Enterprise Solution (Dec. '01/Jan. '02)

DATE:	**November 26, 2001**
ACTION:	**Trilogy UAC Task Order Mod #2**
IMPACT:	**COST (ceiling increase)**

On November 26, 2001 modification #2 was approved to increase the ceiling of CLIN 0003.

CLIN Ceilings

CLIN 1 (Labor)	61,397,931.00
CLIN 2 (Long Dist. Travel)	300,000.00
CLIN 3 (ODCs)	**100,000.00**
CLIN 4	26,063,000.00
Total Contract Value	**87,860,931.00**

DATE:	December 17, 2001
ACTION:	STOP WORK on Web Enabling (Web Enabling began on 10-15-01)
IMPACT:	SCHEDULE (accelerated)
	REQUIREMENTS (stop work)

The support Contractor to the FBI for Trilogy UAC was asked to identify and present several alternatives to accelerate the efforts. The FBI, in conjunction with FEDSIM and the Contractor, determined that "Alternative 2" (which eliminated front end requirements of interim WEB Enablement to the FBI legacy systems) was the best approach to accelerate the schedule. This approach would allow the Contractor to immediately embark on the development of an Enterprise Solution (which has always been the end goal of Trilogy). On December 17, 2001, the FBI requested FEDSIM to provide notification to the Contractor to Stop Work on all WEB Enablement tasks under the Task Order to support Trilogy UAC. **On December 21, 2001,** the Contractor was given PRELIMINARY notification by FEDSIM to Stop Work on tasks C.3.3, Task 3 – Web-Enabled Replacement of User Interfaces; C.3.4, Task 4 – UAC Search Capability, and C.3.14.1, Subtask 14.1 HIS-UWG.

Per discussions with the Contractor, it was agreed that the Stop Work would be for a period of 60 days. During that timeframe a modification would be prepared to restructure the Statement of Work to reflect the elimination of the WEB Enablement tasks and the acceleration of Trilogy UAC.

DATE:	**December 28, 2001**
ACTIONs:	**- Formal "Stop Work" on Web Enabling**
	- Direction to re-focus efforts on Enterprise Solution development
IMPACT:	**SCHEDULE (accelerated)**
	REQUIREMENTS (redirect)

On December 28, 2001, the formal Stop Work notification was provided to the Contractor including a description of the work to be suspended and direction to re-focus their efforts on the remaining Task Order requirements for the development of an Enterprise Solution. In addition, the Contractor was requested to provide documentation identifying the final status of accomplishments to date on the WEB Enablement tasks and to provide a white paper on lessons learned on those efforts.

Based upon the above, issuance of a Stop Work on the identified tasks and entering into a modification by mutual agreement to delete those tasks from the Statement of Work was in the best interest of the Government. This minimized the administrative costs to the Contractor and the Government to realign tasking and costs under the Task Order.

DATE:	**January 25, 2002**
ACTION:	**Authority-To-Proceed on ROM-Based Enterprise Solution**
IMPACT:	**REQUIREMENTS (redirect via an ATP)**

Redirected tasks via an ATP. An ATP was issued in lieu of a modification because Enterprise Solution requirements had not yet been identified in full. Again, ATP was ROM-Based, NOT ECP-Based.

The Contractor was authorized to proceed with the development of the Enterprise Solution. In addition, the ATP letter relayed the intent of proposed modification PS05, which would delete the WEB Enabling tasks and combine the three yearly labor CLINs into a single labor CLIN.

Intent of the Government over the next several weeks was to define the changes to the Task Order and Attachment #5, in order to request a proposal (at that time Attachment #5 was recognized as a "Requirements Document" and is now recognized as an "informational supplement" only). Any adjustments to the task order ceiling would be made in a subsequent modification.

DATE:	**February 8, 2002**
ACTION:	**FBI's Section C/F Revisions Request**
IMPACT:	**REQUIREMENTS (redirect)**

Govt. drafted a contractual redirection in requirements/tasks via section C & F revisions.

On February 8, 2002, the FBI requested FEDSIM to solicit an Engineering Change Proposal (ECP) from the Contractor, to address the accelerated and new direction of the Trilogy UAC program. Changes to section C reflected the shift in FBI direction, which was to strike the task of web enabling FBI legacy systems, and implement an Enterprise Management System (EMS)

solution (changes were based on deletion of web enabling content – no new requirements were added). Changes to section F were also based on deletion of content – no new deliverables were added.

DATE:	**February 19, 2002**
ACTION:	**RFP/ECP Letter Issued to Contractor**
IMPACT:	**REQUIREMENTS (redirect/ECP request)**
Govt. requested a contractual redirection in requirements/tasks via an ECP request.	

FEDSIM requested a technical and cost proposal that would address appropriate changes to Section C and Section F for the accelerated Trilogy UAC Task Order. The Contractor was also invited to address any adjustments to the award fee evaluation criteria for Government consideration. **Proposal deadline was set for March 18, 2002.**

DATE:	**March 5 – May 2, 2002**
ACTION:	**ALPHA Sessions**
IMPACT:	**CONTRACTOR PERFORMANCE (in question)** **COST (BOE justification discussions)** **SCHEDULE (ECP submittal date extended twice)** **REQUIREMENTS (definition discussions)**

Prior to proposal submittal, the government implemented the "Alpha Contracting Approach," which was intended to allow for trade-offs to be evaluated and incorporated into the proposal preparation process. The goal was to receive an acceptable proposal that could be incorporated by task order modification within two weeks following receipt.

Per discussions held during the "March, 2002" Alpha sessions **ECP submittal date was moved to April 12, 2002 (from March 18, 2002).**

Per discussions held during the "April, 2002" Alpha sessions **ECP submittal date was again moved to May 13, 2002 (from April 12, 2002).**

The March and April 2002 Alpha sessions resulted in the Government identification of several "concerns" and "problem areas" in regards to Contractor performance. These concerns/problem areas included, but were not limited to, the following areas:

Contractor was not adequately prepared for Alpha sessions (hand-outs incorrect, managers not prepared, information was inconsistent).
Contractor could not adequately define what work had been accomplished from the ATP issued on January 25, 2002 to the present (end of April, 2002).
Contractor had failed to articulate/justify cost differentials to meet government satisfaction.
Contractor could not adequately define UAC planning of how all function areas were to work in "lock-step" to accomplish Trilogy UAC goals and objectives.
Contractor did not appear to have a strong team (from both leadership and management perspectives) assigned to the Trilogy UAC Task Order.

Because of the above noted concerns and problem areas, the Government considered the following Contractual "Options-to-Proceed:"

Termination for Convenience – Option NOT Exercised

The Government did not view this as a viable option due to justification difficulties (ie. Govt. still has a viable contract need and still has available funding).

Termination by Default – Option NOT Exercised

The Government did not view this as a viable option due to the fact that the Trilogy UAC TOR is a performance based contract. To date, the Contractor had not committed any contractual violations, and there had been no written evaluation/documentation regarding Contractor performance.

Modify Contract to fund "Requirements Analysis" only - Option NOT Exercised

The Government did not view this as a viable option due to the following primary issues:

- Time/Schedule delays to recompete TOR via Millennia or Millennia Lite
- Time/Schedule delays due to learning curve of a new Contractor
- Political ramifications (Congressional expectations already established on the Hill)

Mutual Agreement to establish "ending period" with Contractor - Option NOT Exercised

Per above (Option 3), FEDSIM CO recommended this approach, if the Government chose to "de-scope" requirements/tasking efforts. For the same reasons noted above (Option 3), the Government did not view this as a viable option.

FIX IT (Continue with proposal negotiations) - OPTION EXERCISED

BOTTOM LINE, in order to maintain a good working relationship with the Government, the Contractor needed to:

Build confidence (with the Government)

Strengthen the Team (replace applicable personnel in order to provide better management and leadership).

DATE:	**May 13, 2002**
ACTION:	**Contractor's ECP Received**
IMPACT:	**COST (program over budget)**

Total program cost of the Trilogy UAC ECP exceeded funding in FBI's allocated budget for the Trilogy UAC program.

Available funding to the FBI was approximately: $108M
Contractor Cost Proposal was approximately: $149M

DATE:	June 24, 2002
ACTION:	Trilogy UAC Mod #8
IMPACT:	COST (ceiling increase)

On June 24, 2002 modification #8 was approved to increase CLIN 0003 ceiling.

CLIN Ceilings

CLIN 1 (Labor)	61,397,931.00
CLIN 2 (Long Dist. Travel)	300,000.00
CLIN 3 (ODCs)	**150,000.00**
CLIN 4	26,063,000.00
Total Contract Value	**87,910,931.00**

DATE:	July 9, 2002
ACTIONs:	- FEDSIM requests revised ECP (ECP1a) from Contractor - Revised/Updated Authority-to-Proceed (ATP) issued to Contractor IMPACT: COST (budget constraints) SCHEDULE (budget constraints) REQUIREMENTS (budget constraints) Revised/updated tasks via an ATP. An ATP was issued in lieu of a modification because Enterprise Solution requirements had not yet been identified in full.

As noted earlier, the FBI did not have sufficient funding allocated to fund the Trilogy UAC program in its entirety, at this time. In order to best assist the FBI, FEDSIM requested a revised ECP (ECP01a for work through November 30, 2002). It was/is also the desire of the government to award additional ECP(s), as needed, to continue performance beyond November 30, 2002, dependent upon the FBI's available budget.

On July 9, 2002, FEDSIM requested a revised technical and cost proposal, ECP01a, (from the original ECP01, received on May 13, 2002) and provided a revised/updated ATP for work performed, prior to execution of a modification incorporating the negotiated ECP01a.

The ECP01a proposal deadline was set for July 26, 2002.

DATE:	**July 26, 2002**
ACTION:	**Contractor's ECP1a Received**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS**

Contractor provided ECP1a to the Government which was a revision of the ECP proposal received on May 13, 2002. However the cost and technical proposal now reflected a period-of-performance (PoP) through November 30, 2002 only (not entire duration of anticipated PoP).

Contractor Cost Proposal was approximately: $67M (6/5/01 – 11/30/02)

DATE:	**August, 2002 – October 10, 2002**
ACTION:	**Award Fee Negotiations**
IMPACT:	**CONTRACTOR PERFORMANCE** **COST (fee negotiated/invalid performance criteria)** **SCHEDULE (ECP1a Mod Delayed)**
Award Fee had to be negotiated due to invalid performance criteria for periods 1 and 2 (resulting from 9-11 terrorist attacks).	

ECP1a could not be implemented contractually (via modification), until all parties (FBI, FEDSIM and the Contractor) completed/reached concurrence on negotiations for the Trilogy UAC Award Fee distribution/plan. Mutual agreement was reached on October 10, 2002 by all parties on the following points (with a proposed revision of the Award Fee Determination Plan to be forwarded by the FBI):

$1,267,000 negotiated fee amount for the 1st and 2nd award fee periods.
3% base fee and 7.5% award fee pool for period 3 (end date of November 30, 2002)
ECP01b delivery 1 award fee will be allocated as follows:
- 3% base fee and 7.5% award fee pool if delivery 1 occurs on or before December 12, 2003.
- 3% base fee and 8.5% award fee pool if delivery 1 occurs on or before November 12, 2003.
- 3% base fee and 9.5% award fee pool if delivery 1 occurs on or before October 12, 2003

If the options are exercised, the same award fee structure will apply for deliveries 2 and 3.
In the ECP01b award fee period, the contractor may earn all, part, or none of the award fee allocated to the applicable evaluation periods. If the award fee rating is 80 or higher, then any unearned award fee will automatically roll over into a subsequent award fee period. For award fee ratings below 80, the AFDO reserves the right to make a determination as to the amount of unearned award fee, if any, to be rolled over into a subsequent period.

DATE:	**October 10, 2002**
ACTION:	**FEDSIM Requests ECP1b from Contractor**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS**

FEDSIM requested ECP01b which would provide cost/schedule for the Trilogy UAC program **in its entirety** (projected to end August, 2004).

The ECP01b proposal deadline was set for October 30, 2002.

DATE:	**November 4, 2002**
ACTION:	**Contractor's ECP01b Received**
IMPACT:	**COST (program still over approved budget)** **SCHEDULE** **REQUIREMENTS**

Contractor provided a cost and technical proposal for the Trilogy UAC program in its entirety (projected to end August, 2004). Total program cost of the Trilogy UAC ECP01b still exceeds FBI's allocated budget for the Trilogy UAC program. However, the FBI was confident that additional funding would be secured.

Contractor Cost Proposal is approximately: $141M (6/5/01 – 8/2004)

DATE:	**December 5, 2002**
ACTION:	**Trilogy UAC Task Order Mod #12 (ECP1a Complete)**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS**

SAIC's proposal dated May 13, 2002 (ECP), as revised on July 26, 2002 (ECP01a) and October 17, 2002 (ECP01a) is incorporated by this modification. The proposal iteration dated October 17, 2002, covers anticipated costs from date of award through December 6, 2002 (in lieu of through November 30, 2002 as captured in the July 26, 2002 proposal). The December 6 date represents the end date for Award Fee period 3.

SAIC's letter dated December 4, 2002, is incorporated by reference and this modification authorizes work to be performed IAW with that letter. Funding currently obligated under the

Task Order covers costs incurred to date, as well as anticipated expenditures to be incurred IAW the December 4th letter through December 31, 2002.

Section C was modified to reflect the following:

- Delete the WEB enabling tasks
- Add Section 508 requirements
- Add requirements to re-engineer the data and business processes
- Create a single physical database
- Build custom applications and software around user requirements
- Overhaul the security and access control mechanisms

Section F was modified to do the following:

- Extend the period of performance from June 2004 to August 2004 and to specify the delivery date for delivery 1 deployment to be December 12, 2003
- Modify the milestone schedule for additional planned completion dates for deliverables and activities planned to date
- Modify the specifications for the Trilogy UAC master plan

Section J was modified to re-define the Award Fee Determination Plan and to add accessibility standards IAW 508.

DATE:	**April 7, 2003**
ACTION:	**Authority-To-Proceed on ECP1b Options 1 and 2**
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS (redirect in approach)
	***VISION/APPROACH CHANGE (as proposed by SAIC/agreed to by Gov)**
The previous ATP issued in conjunction with ECP01a, Mod #12, on December 5, 2002, anticipated an earlier ECP01b contract modification timeline.	
***This could be considered a key data point where the vision/approach of the VCF program shifts from clear cut integration and replacement of the five major existing (legacy)**	

Schedule Concerns: Actual timeline (as opposed to anticipated timeline) necessitated a need to update ATP activities in order to preserve schedule, since the previous ATP issuance did not reflect start up activities on Options 1 and 2 of the ECP01b proposal.

Budget Concerns: A modification could not be issued at this time because the total program cost of the Trilogy UAC program (as proposed in ECP01b) still exceeded funding in FBI's allocated budget. Additional Trilogy UAC reprogramming dollars had not yet been approved by Congress.

VCF Vision: This ATP letter also recognized a new product management approach (as proposed by SAIC/agreed to by the Government). As the vision of the VCF emerged, the VCF team began to recognize the implications of this new enterprise system and how the FBI will do business in the future. **The plan to simply migrate three more systems into the VCF environment does not acknowledge that the previously envisioned "target" system has changed dramatically since the Delivery 2 and 3 plan was originally developed.** FEDSIM and the FBI agreed with

SAIC that a product management approach for developing the VCF as well as other enterprise-level applications should be considered.

DATE:	**May 16, 2003**
ACTION:	**GSA/FEDSIM issues Award Fee amount for Period 3**
IMPACT:	**AWARD FEE/COST**
	CONTRACTOR PERFORMANCE (87% final rating – out of possible 100%)

- Final award fee performance evaluation report and determination amount for period 3 was forwarded to SAIC. **This resulted in a 87% performance rating** (out of 100% possible rating).
- SAIC awarded 87% of the monies available for Trilogy UAC award fee period three (06/22/02 – 12/06/02).
- SAIC awarded a fee of $932,758.00, and all of the unearned fee of $139,378.00 was rolled forward from the third award fee period to the fourth award fee period.

DATE:	**June 20 – June 24, 2003**
ACTION:	**ALPHA Sessions – Revisited for ECP1b**
IMPACT	**COST (BOE justification discussions)**
	SCHEDULE (justification discussions)
	REQUIREMENTS (definition discussions)

Alpha pricing sessions were again conducted with the Contractor to revisit the basis of estimates (BOEs) for the ECP1b cost proposal. This proposal had not changed since submission on November 4, 2002 and due to delay in issuance it was deemed necessary by the Government to revisit this proposal. Technical requirements were also discussed in the context of the required technical skills and level of effort required to accomplish the tasks required by the statement of work. Any inconsistencies found in the BOEs (regarding current status gameplan as to what was proposed in November of 2002) were resolved during these sessions.

Only changes from ECP1b proposal were:

- Multi Media Station Training
- BOE – 1.6.6 (Data Engineering)
  - SAIC update (re: task description w/ 4,193 hrs)
  - SAIC replaced Nov 02 BOE (1.6.6 & 1.6.7) with Feb 03 replan (new 1.6.6)
- BOE 1.10 (Training)
  - SAIC striked training hours as identified in ECP01b BOE notebook (pg. 454)
  - SAIC updated training materials and delivery of training

DATE:	**July 18, 2003**
ACTION:	**Contractor at Risk (Start Date)**
IMPACT:	**COST**

The Contractor was now working at risk because the Trilogy UAC program had reached the ceiling level on CLIN 0001 - Labor ($61M). FEDSIM could not increase the ceiling (via a modification incorporating ECP01b) because Congress had still not approved additional Trilogy reprogramming dollars.

Contractor performed "at risk" (July 17, '03 - Sept. 4 '03) during this period even though future funding for the Trilogy UAC program was still unknown/unapproved.

DATE:	July 31, 2003
ACTION:	Senate approves Trilogy Reprogramming Dollars
IMPACT:	COST

On 7/31/03 the Senate approved $110M out of the $138M Trilogy reprogramming dollars sought/requested by the FBI.

DATE:	September 2, 2003
ACTION:	FEDSIM Receives Trilogy Reprogramming Dollars
IMPACT:	COST

The Treasury Department forwarded approved funding to the FBI on August 29, '03. FEDSIM received $53.1M of FBI funding to obligate on Trilogy UAC on September 2, 2003.

Contractor was still at risk (since July 18, '03).

DATE:	September 4, 2003
ACTION:	Trilogy UAC Mod #22 (ECP1b Complete)
IMPACT:	COST (ceiling increase)
	SCHEDULE
	REQUIREMENTS

Modification #22 incorporated by reference SAIC Engineering Change Proposal (ECP) No. 01b into this Task Order. ECP 01b consists of Part I (Cost Proposal), Part II (Technical Proposal) and Part III (Basis of Estimate) dated 4 November 2002, revised July 2003, and approved/accepted by the Government on July 25, 2003.

Modification #22 increased, as well as **funded Trilogy UAC CLINs 1, 2 and 3 in their entirety.**

CLIN Ceilings

CLIN 1 (Labor)	113,035,239.00
CLIN 2 (Long Dist. Travel)	542,115.00
CLIN 3 (ODCs)	916,218.00
CLIN 4	27,264,000.00
Total Contract Value	141,757,572.00

DATE:	September 21, 2003
ACTION:	Award Fee Period 4 – Interim Performance Evaluation #1
IMPACT:	AWARD FEE
	CONTRACTOR PERFORMANCE (75% interim rating – out of possible 100%)

Award Fee Evaluation Report (number 1) for period 4 was forwarded to the contractor. This report served as a "checkpoint" to clarify the Government's current position of the Contractor's performance rating/score for award fee period 4.

- **Contractor Performance Points: 75 (out of 100 possible)**
- **Contractor Rating Adjective: Standard** (Award Fee Point Range – 70 to 79)
- **Standard is defined as:** *Performance meets Task Order requirements. Non-conformances are minor, but Government resources are required to assure that timely corrective actions are taken. Customer satisfaction is at risk.*

CRITERIA	Rating Adjective	Points	Weight (%)	Category Total
Technical	Standard	74	40%	30
- Test	- Marginal	- 62	- 10%	
- Training	- Standard	- 70	- 10%	
- System Design	- Standard	- 73	- 10%	
- System Support	- Good	- 90	- 10%	
Schedule	Standard	75	40%	30
Cost	Standard	75	20%	15
GRADE	Standard			75
Award Fee				N/A for now
Roll Over				N/A for now

DATE:	**December 2, 2003**
ACTION:	**Award Fee Period 4 – Interim Performance Evaluation #2**
IMPACT:	**AWARD FEE**
	CONTRACTOR PERFORMANCE (69% interim rating – out of possible 100%)

Award Fee Evaluation Report (number 2) for period 4 was forwarded to the contractor. This report served as a "checkpoint" to clarify the Government's current position of the Contractor's performance rating/score for award fee period 4.

- **Contractor Performance Points: 69 (out of 100 possible)**
- **Contractor Rating Adjective: Marginal** (Award Fee Point Range – 61 to 69)
- **Marginal is defined as:** *Nonconformances are serious, and extra Government resources are required to assure that corrective actions are taken. Few achievements are made. Contractor is not proactive. Corrective actions are not timely or effective. Customer is not satisfied.*

CRITERIA	Rating Adjective	Points	Weight (%)	Category Total
Technical	Marginal	67	40%	27
- Test	- Unsatisfactory	- 42	- 10%	
- Training	- Standard	- 79	- 10%	
- System Design	- Unsatisfactory	- 56	- 10%	
- System Support	- Good	- 90	- 10%	
Schedule	Standard	70	40%	28
Cost	Standard	70	20%	14
GRADE	Marginal			69
Award Fee				N/A for now

Roll Over N/A for now

DATE:	**December 3, 2003**
ACTION:	**Trilogy UAC Mod #24**
IMPACT:	**COST (ceiling increase)**
	REQUIREMENTS

Modification #24 authorized an increase in the number of facilitated instructors for Virtual Case File (VCF) training from 25 to 60. The reason for this increase is to ensure there is enough training coverage to send facilitators to all field offices (FOs) and resident agencies (RAs). This change request (CR-0308) was approved through SAIC's Engineering Review Board (ERB), the SAIC Configuration Control Board (CCB) and the FBI.

CLIN Ceilings

CLIN 1 (Labor)	**114,033,095.00**
CLIN 2 (Long Dist. Travel)	**1,167,217.00**
CLIN 3 (ODCs)	916,218.00
CLIN 4	27,264,000.00
Total Contract Value	**143,380,530.00**

DATE:	**December 11, 2003**
ACTION:	**Arbitration Process Meeting**
IMPACT:	**COST (increase labor CLIN ceiling vs. bill against labor CLIN ceiling)**
	REQUIREMENTS (FEDSIM to arbitrate disputes)

The growing number of new Change Requests (CRs) that were impacting cost now required 3rd party intervention to deem applicable CRs as either a CHANGE (NEW Requirement) OR a FIX.

- A **FIX** is a change designed to bring the system into compliance with a specified set of functional (or physical) requirements.
- **CHANGES** are those related to improving performance, or capabilities, beyond the minimum requirements stated in the specification.

Changes with associated cost impact are treated as a new requirement (new cost/increase in ceiling) and fixes are billed against the "current" ceiling.

All parties (FBI, FEDSIM and SAIC) agreed to implement an arbitration process to solve disputes over interpretation of changes vs. fixes within the VCF program. One primary POC was appointed from each party (FBI, FEDSIM and SAIC) in this arbitration process. FEDSIM has final ruling authority on those issues that do not reach agreement/concurrence between the FBI and SAIC. This process is held independently from the current CR and Software Problem Reports (SPR) processes.

DATE:	**December 12, 2003**
ACTION:	**VCF Deployment Date Not Met**
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS

The contractor failed to deploy the VCF system upon the agreed deployment date of December 12, 2003.

DATE:	**December 17, 2003**
ACTION:	**VCF System Delivered (NOT Deployed) to the Government**
IMPACT:	**SCHEDULE**
	REQUIREMENTS

VCF System was delivered (NOT deployed) to the Government on Wednesday, Dec. 17, 2003.

DATE:	**January 21, 2004**
ACTIONs:	**- FEDSIM rejects 12-17-03 VCF delivery**
	- Gov cites 17 VCF deficiencies
	- Gov request: When will VCF be delivered for inspection/acceptance?
	- Gov request: Will SAIC complete program at or under cost, within PoP?
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS (VCF rejected)

A "draft" VCF system had not been recognized as a contractual Section F deliverable by the Government.

- FEDSIM issued written correspondence to inform SAIC that **the Virtual Case File as delivered on December 17, 2003 was not acceptable** (in accordance with FAR 52.246-5, Inspection of Services – Cost Reimbursement).
- In accordance with Millennia Contract GS00T99ALD0210, Section E 3.3, the Government also provided written notification citing **17 deficiencies addressing why the VCF system/deliverable was not considered acceptable.**
- SAIC was authorized to perform activities necessary to address the 17 deficiencies.
- SAIC was requested to provide written notification of when they anticipated VCF to be delivered for inspection/acceptance.
- Finally, SAIC was requested to provide written response if SAIC expected to complete Delivery 1, Release 2 and Release 3 within the current Period of Performance (June 5, 2001 – August 2, 2004) at or under the current contract ceiling of $143,380,530.

DATE:	**January 23, 2004**
ACTIONs:	**- SAIC deems 12-17-03 VCF delivery a DRAFT submission**
	- SAIC responds to 17 deficiencies
	- SAIC provides acceptance date for VCF
	- SAIC provides VCF completion date/cost/schedule
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS

- SAIC responded to FEDSIM via written correspondence indicating the VCF delivery of December 17, 2003 was a **draft submission, not final**.
- In regards to the 17 deficiencies, SAIC indicated that they believed a number of the items within the list were **changes to the specification** and **not deficiencies**.
    - FEDSIM would work independently (as agreed to via the Dec. 11 2003 Arbitration Process meeting) to review all 17 issues (and sub-issues) and make a determination for final ruling that would deem each item as either a change/new requirement OR a fix. In parallel, SAIC would move forward to complete necessary design activities that addressed all 17 identified issues (and sub-issues).

- SAIC developed/submitted a schedule that estimated the following major acceptance milestones as follows:

    - **Complete System Test** – April 26, 2004
    - Complete preparations for Acceptance Test – May 10, 2004
    - **Ready for Acceptance Test** – May 11, 2004

- SAIC updated the resource-loaded network (RLN) which now indicated a**expected completion date of October 29, 2004 for all project activities.**
- In regards to cost, SAIC indicated that **they did not anticipate exceeding the current task order ceiling of $143M**. However, SAIC did estimate that CLIN 0001 (Labor) would exceed the current CLIN ceiling by $14.2M (exclusive of base and award fee) and that CLIN 0004 (Tools) would under-run current CLIN ceiling by $25M.
- **SAIC estimates only addressed work scope authorized under the task order as currently modified.** Outstanding Change Requests (CRs) for the Production Performance Test and the Training Environment were not considered in these cost and schedule estimates. In addition, unauthorized or undefinitized activities, still under consideration by FEDSIM and the FBI, had not been included in this estimate. Some of these activities included Section 508 implementation, Instructor-led training (ILT) activity, changes to the Training Environment, User Acceptance, Beta Testing, additional TNC/IPC integration testing, and Records Management Application (RMA) changes.

DATE:	**February 9, 2004**
ACTIONs:	**- FEDSIM again confirms rejection of 12-17-03 VCF delivery** **- FEDSIM does not recognize "draft" VCF system as a deliverable** **- Gov deems VCF delay unjustified** **- Gov requests Estimate-To-Complete (ETC) for D1 and R2/R3** **- Gov captures 16 items for scope clarification**
IMPACT:	**COST** **SCHEDULE (delay unjustified)** **REQUIREMENTS (contractual validity of VCF draft)**

- FEDSIM informed SAIC via written correspondence that per the ECP01b modification agreement of September 4, 2003, the VCF system was proposed to be delivered to the Government on December 12, 2003, for deployment. The VCF was not delivered in a state ready to be deployed, and had not been provided to the Government for User Acceptance and Testing in accordance with SAIC's proposed schedule on October 20, 2003. **Therefore, the VCF as delivered on December 17, 2003 was not acceptable.**
- FEDSIM communicated the Government's position that the delayed availability of TNC/IPC did not prevent SAIC from completing development and initial application testing of the VCF. Because there were no dependencies on the TNC/IPC schedule for development and "delivery" of the VCF, **the Government did not find acceptable justification for an excusable delay.**
- **The Government requested SAIC to provide an Estimate to Complete (ETC)** for Delivery 1, Release 2 and Release 3, in accordance with ECP01(b).
- **The ETC deadline was set for February 13, 2004.**
- 16 activities were noted for inclusion with this ETC direction. The 16 Activities captured were:

    1. Records Management Application (RMA)
    2. Security

3. Interface Testing
4. Data Engineering
5. Acceptance Test Criteria
6. IPC/TNC task order visibility
7. Acacia document needs
8. Training Delivery Approach
9. Performance testing using the production system infrastructure
10. Operations and Maintenance approach
11. ArcSight
12. Section 508
13. Implementation of CISP/Intelplus functions and data migration
14. VCF maintenance releases
15. EOC Support
16. Improvement in SAIC Test Cases

DATE:	**February 10, 2004**
ACTIONs:	**- SAIC again defends 12-17-03 VCF delivery as a DRAFT submission** **- SAIC defends Mgt. practices in communicating VCF schedule slippage** **- SAIC requests face-to-face discussions for ETC scope clarification** **- SAIC cites 28 outstanding CRs (w/cost impacts) for ETC clarification**
IMPACT:	**COST** **SCHEDULE (communication of slippage)** **REQUIREMENTS (contractual validity of VCF draft)**

- SAIC's correspondence again defends VCF delivery of December 17, 2003 as a draft deliverable and also defends SAIC's management practices regarding the communication to the Government on VCF schedule status (re: slippage).
- SAIC requests face-to-face discussions in order to reach agreement on full scope/clarification of all ETC related activities.
- SAIC recognized 28 Change Requests (CRs) that had been jointly reviewed and approved by the FBI via the Configuration Control Board (CCB) that still required cost/schedule impact proposals for modification.

DATE:	**February 12, 2004 – March 22, 2004**
ACTION:	**ETC Scope Clarification Activities/Discussions**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS (define ETC)**

ETC scope clarification discussions were kicked off at the SAIC Vienna facility on February 12 (all day event). Over 100 items were captured/discussed that required attention for ETC clarification purposes.

Closure processes for all recorded activities that required clarification for ETC issuance would take the VCF program through March 22, 2004 (date of revised ETC issuance from FEDSIM).

DATE:	**February 13, 2004**
ACTIONs:	**- Gov descopes IntelPlus requirement** **- Gov suspends R2/R3 activities**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS (descope/stop work)**

- The Government requested SAIC to continue development of Delivery One with the exception of the IntelPlus application functionality and data migration. SAIC was now to provide only an interface to the IntelPlus legacy application as part of Delivery 1.
- The Government also requested SAIC to suspend all development and related activities for Releases 2 and 3. The only exception to this directive was the Evidence Program Audit Inventory Software (EPAIS), which the Government requested to include as part of Delivery 1.

DATE:	**March 12, 2004**
ACTION:	**Award Fee Period 4 – Final Evaluation and Award Fee Determination**
IMPACT:	**AWARD FEE/COST** **CONTRACTOR PERFORMANCE** **(34% final period rating–of possible 100%)**

Final award fee performance evaluation report and determination amount for period 4 was forwarded to SAIC. This resulted in a 34% performance rating (out of a possible 100%), $0.00 earned in award fee, with 100% roll over for period 4.

- **Contractor Performance Points: 34 (out of 100 possible)**
- **Contractor Rating Adjective: Unsatisfactory** (Award Fee Point Range – 0 to 60)
- **Unsatisfactory is defined as:** *Nonconformances are serious, and extra Government resources are required to assure that corrective actions are taken. Few achievements are made. Contractor is not proactive. Corrective actions are not timely or effective. Customer is not satisfied.*

CRITERIA	**Rating Adjective**	**Points**	**Weight (%)**	**Category Total**
Technical	Unsatisfactory	44	40%	18
- Test	- Unsatisfactory	- 30	- 10%	
- Training	- Unsatisfactory	- 60	- 10%	
- System Design	- Unsatisfactory	- 28	- 10%	
- System Support	- Unsatisfactory	- 57	- 10%	
Schedule	Unsatisfactory	20	40%	8
Cost	Unsatisfactory	40	20%	8
GRADE	Unsatisfactory			34
Award Fee				$0.00
Roll Over				100% roll over

DATE:	**March 12, 2004**
ACTION:	**FEDSIM Issues Final Determination Ruling on 17 VCF "Deficiencies"** **Modification PS25 incorporates this understanding**
IMPACT:	**COST (increase ceiling OR bill against ceiling)** **REQUIREMENTS ("deficient" OR "new work")**

FEDSIM completed independent review to resolve SAIC/FBI dispute over each party's position (change OR fix) on the 17 issues cited in the Government's January 21, 2004 correspondence regarding VCF acceptance.

FEDSIM issued the final ruling to all parties, defining each issue as a change or fix, with applicable justification. Final results captured the following break-down of the 17 issues (and applicable sub-issues under each of the 17, totaling 59 items in all):

- Changes 19
- Fixes 40

DATE:	**March 22, 2004**
ACTION:	**FEDSIM issues Second Request for ETC (per post ETC definition activities/discussions) from Contractor**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS (ETC definition discussions closed)**

Parties reached closure on ETC activities that required clarification/definition.

FEDSIM requested an ETC from SAIC which would provide cost/schedule for Delivery 1, Release 2 and Release 3, as agreed to in ECP01b for the User Application Component (UAC).

The ETC deadline was set for April 2, 2004.

DATE:	**March 22 – April 1, 2004**
ACTION:	**VCF Functional Review Sessions**
IMPACT:	**REQUIREMENTS (functional validation)**

VCF Functional review sessions ran in parallel with ETC costing and scheduling activities (as opposed to completing PRIOR to ETC activities). Due to time constraints, all parties recognized, agreed to, and accepted the risk involved with this parallel approach (all parties understood that results of these sessions could significantly impact SAIC's ETC submittal package).

SAIC conducted 8 separate VCF Functional Review sessions during this time period with intent to demonstrate to the Government how the VCF system would fulfill the functionality needed to support the FBI's business. Processes included SAIC to walk the Government through predetermined investigative business scenarios/transactions as conducted using the VCF system. **Approximately 400 issues were captured for further Government review/direction during this 2 week functional review period.**

Gameplan for NEXT STEPs beyond VCF Functional Review included:

1. SAIC review of the 400 issues and to identify FIXES (as opposed to changes/new requirements)
2. FBI review of the 400 issues to cite concurrence or non-concurrence on FIXES identified by SAIC
3. FBI review of the 400 issues to identify SHOWSTOPPERs for D1 ("must haves")
4. FBI review of the 400 issues to identify which issues would be included for future maintenance releases (follow-on from D1)
5. **DESCOPE:** Per ETC cost and schedule, FBI to review 400 issues to identify what could be deferred/must be deferred from D1

DATE:	**March 23, 2004**
ACTION:	**FEDSIM Extends ETC Deadline**
IMPACT:	**COST** **SCHEDULE** **REQUIREMENTS**

The ETC deadline was extended to April 7, 2004.

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

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

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

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

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

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

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

ETC Submission reflected the following data:

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

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

Schedule:

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

Key Items:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Provisional Program deadline was set for May 26, 2004.

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

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

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

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

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

The Government proposed the following **deployable capabilities** to SAIC:

- Leads Management
- Case Management
- Document Management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Attachment 1** - Identified those functional areas that would not be operational in IOC (list drafted by the FBI – previously reviewed by SAIC)
- **Attachment 2** - Identified those non-IOC activities from the 14 April 04 ETC (list was developed via a 7 June 04 working meeting between SAIC and FBI)

- **The Government also requested SAIC to stop work on all data migration activities**, with the exception of support for the data migration staging database (normalized version of ACS residing on ORACLE) which would include:
    - Extraction of data from the ACS application to populate the staging database
    - Synchronize data updates between the ACS application and the staging database
    - Analyze data error conditions and provide reports describing these conditions, including level of severity and alternatives for resolution

- **The Government also requested SAIC to stop work on all non IOC-related Software Problem Reports (SPRs) and Test Cases** (per review and identification activities to clarify any IOC relation).
- **The Government also requested SAIC to stop work on the Delivery 1 Test Plan.**
- **The Government also requested SAIC to provide a revised estimate of funds expenditure date** (revised "burn rate") based on this directive by June 14, 2004.

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

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

- SAIC letter confirmed that the affected project personnel stopped work on the identified activities as of COB Friday, June 11, 2004.

- SAIC identified two areas of work that should be continued (as captured in their correspondence, verbatim):

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

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

- SAIC also requested clarification on the direction to continue some elements of the data migration activities.

- SAIC reduced its staff by a total of fifty-five (55) (including subcontractor personnel) as a result of the Stop Work Order. This reduction in staff changed the funds expenditure date to June 18, 2004.

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

DATE:	**June 15, 2004**
ACTION:	**Agreement between Director Mueller and CEO of SAIC**
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS

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

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

DATE:	**June 18, 2004**
ACTION:	**Modification to realign funding**
IMPACT:	**COST**

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

DATE:	**June 28, 2004**
ACTION:	**FEDSIM issues RFP to SAIC for VCF IOC**
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS

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

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

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

SCHEDULE:

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

TRILOGY UAC ACCOMPLISHMENTS SINCE MARCH 19, 2004:

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

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

DISPOSITION:

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

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

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

DATE:	**July 29, 2004**
ACTION:	**Modification PS28**
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS

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

DATE:	**July 29, 2004**
ACTION:	**Modification PS29**
IMPACT:	**COST**
	SCHEDULE
	REQUIREMENTS

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

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

• Provide incremental funding.

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

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

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

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

• Provide incremental funding

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

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

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

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

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

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

DATE:	**17 January 2005**
ACTION:	**Modification PO36**
IMPACT:	**COST**

- Provide incremental funding

LIVE DOCUMENT NOTE

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

SUBMISSIONS FOR THE RECORD

UNITED STATES SENATOR • IOWA

CHUCK GRASSLEY

http://grassley.senate.gov
grassley_press@grassley.senate.gov

Contact: Jill Kozeny, 202/224-1308
Beth Pellett, 202/224-6197
Dustin Vande Hoef, 202/224-0484

For Immediate Release
Thursday, May 20, 2004

Letter Questions Performance of FBI's Legal Attache Office in Saudi Arabia

WASHINGTON — Sen. Chuck Grassley, a long time critic of the FBI, has requested information and special reviews of the FBI Legal Attache Office in Riyadh, Saudi Arabia. Grassley, chairman of the Senate Finance Committee, made the request along with Sens. Max Baucus, ranking member of the Senate Finance Committee; Orrin Hatch, chairman of the Senate Judiciary Committee; and Patrick Leahy, ranking member of the Senate Judiciary Committee.

"The performance of this office in particular is critical. We need to know how Saudi Arabia is helping us fight the war on terror. If the FBI's Legat in Riyadh is sub-par, we've got problems," Grassley said.

Grassley's oversight of the FBI began in the early 1990's. He has focused on the FBI's internal disciplinary problems in recent years after revelations of senior officials committing misconduct and escaping accountability through a double standard in discipline. He's also been concerned with the FBI's inability to prevent crime and terrorism rather than just investigating crimes after they have occurred.

Here is the letter.

May 19, 2004

The Honorable Robert Mueller
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Dear Director Mueller:

We are writing to inquire and express concern about the Federal Bureau of Investigation's (FBI) Legal attache office (Legat) in Riyadh, Saudi Arabia. Specifically, we request that you provide

copies of any and all Inspection Division reports, including special reviews, conducted of the Riyadh Legat office since it opened.

The performance of that office and its personnel has come to our attention for a number of reasons. Saudi Arabia's relationship to the United States is an important one, as is the FBI's relationship to its counterparts in Saudi Arabia. These Saudi security agencies have a wealth of intelligence and terrorism information that can be of great use to the FBI. At the same time, since the terrorist attacks of September 11, 2001, significant and alarming information has come to light about alleged support for terrorism by Saudi Arabian individuals and organizations. In particular, the Senate Finance Committee is investigating terrorism financing, including the sources of funds, methods to distribute monies, and the performance of relevant agencies. Reported involvement by Saudi Arabian individuals and entities is a particular focus of the ongoing investigation. At the same time, the Senate Judiciary Committee continues to investigate allegations of retaliation and a double standard in discipline at the FBI. Agent Bassem Youssef, who has made such allegations, was interviewed by committee staff with FBI authorization. Agent Youssef was assigned to the Riyadh office from February of 1997 to June of 2000. Shortly after his departure, the performance of the office and its new personnel was called into question. We understand that at least one, and perhaps more than one, special inspection team was dispatched to investigate and evaluate the office's performance, separately from the periodic inspections of field offices and Legats.

It is our responsibility to conduct oversight of these issues and investigate and evaluate these reported problems, especially when the issues are of such public concern. Reviewing the inspection reports of the Riyadh Legat office is a crucial step in this effort. It is our understanding that these reports are almost entirely unclassified. If any portions are classified, we ask that they be delivered to the Office of Senate Security for review by us and our staff with clearance. Unclassified versions should be delivered to our offices.

Because this information is readily available for delivery and does not require research, we ask that you provide this information by Wednesday, June 9, 2004. We thank you in advance for your cooperation.

Sincerely,

Charles E. Grassley
CHAIRMAN
COMMITTEE ON FINANCE

Max Baucus
RANKING MEMBER
COMMITTEE ON FINANCE

Orrin Hatch
CHAIRMAN
COMMITTEE ON JUDICIARY

Patrick Leahy
RANKING MEMBER
COMMITTEE ON JUDICIARY

News Release

JUDICIARY COMMITTEE

United States Senate • Senator Orrin Hatch, Chairman

May 20, 2004 Contact: Margarita Tapia, 202/224-5225

Statement of Chairman Orrin G. Hatch
Before the United States Senate Judiciary Committee
Hearing on

"FBI OVERSIGHT: TERRORISM AND OTHER TOPICS"

Today we will conduct an oversight hearing on the FBI's efforts to combat terrorism as well as other issues. I would like to welcome FBI Director Robert Mueller, who will testify before us today. I enjoyed our meeting earlier this month, which I thought was very productive.

As many of you know, Director Mueller started his job one week prior to 9/11. At the time, although the FBI was the subject of intense criticism and media coverage, Director Mueller was undaunted and took the job head on. Over the last three years, he has accepted the challenge of transforming the FBI and has made every effort to help usher the FBI into the 21st Century. The challenges that he has undertaken are ambitious and, of course, cannot be completed overnight.

In an agency that has 56 field offices, over 400 satellite offices, 52 overseas offices and employs over 28,000 people, it is impossible to know what is going on in every place at every moment. Yet Director Mueller has made it his business to find out where the trouble spots are and to take every measure to resolve problems, investigate any misconduct, and to seek outside expertise, when necessary to assess or address the issue.

One of the many aspects of Director Mueller's performance that I continue to be most impressed by is how responsive he has been to Congressional concerns. Let me give you one example. I know my friend and colleague from Vermont is diligent in making sure that witnesses that have appeared before the Judiciary Committee on prior occasions have answered their written questions. As I am sure Senator Leahy appreciates, Director Mueller has made sure that *every* written question posed to the FBI at the last oversight hearing was answered.

The FBI's number one priority since 9/11 has been to protect the American people from another terrorist attack. In the subsequent two years and eight months, the FBI has succeeded in that goal. Since September 11, 2001, more than 3,000 Al Qaeda leaders and foot soldiers have been taken into custody around the globe; nearly 200 suspected terrorist associates have been charged with crimes in the United States, and as many as a hundred terrorist attacks or plots have been broken up worldwide.

As we all know, before September 2001, we had communications challenges between the law enforcement community and the intelligence community. Sections 203 and 218 of the USA PATRIOT Act—which are due to expire on December 31, 2005—have been instrumental in breaking down the artificial wall of non-communication between the intelligence community and the law enforcement community. We will never forget the joyous occasion of the fall of the Berlin Wall on November 9, 1989. Anytime walls come down allowing for growth and greater achievement, it is momentous. The wall that came crumbling down with the passage of the USA PATRIOT Act has great significance for those in the law enforcement and intelligence communities. By facilitating and encouraging increased communication among federal agencies, the USA PATRIOT Act has paved the way for many of the coordination initiatives that Director Mueller has undertaken.

Perhaps the greatest consequence of the tearing down of the wall is that it has set the stage for a new culture of cooperation within the government. Before 9/11, federal, state and local agencies tended to operate individually. They were territorial, wanting to preserve their own jurisdiction, and not used to sharing information and resources. I think 9/11 was a wake up call for all of us. It became clear that we needed to establish task forces to coordinate information and work cooperatively to share intelligence and law enforcement leads in order to effectively fight this war on terror.

It takes time to change long-held cultural mores, and to ensure that everyone is sharing information when they should, but Director Mueller has taken several key steps in the right direction. Today, the FBI and the CIA are integrated at virtually every level of operations. Under Director Mueller's leadership, the FBI created the National Joint Terrorism Task Force, which works with the FBI's newly created Office of Intelligence to coordinate inter-agency intelligence-gathering activities and to act as a liaison between FBI Headquarters and local JTTFs.

At the direction of the President, the FBI is leading the effort on the Terrorist Screening Center, which became operational last December. The FBI is also involved in the Terrorist Threat Integration Center, which was established last May at the direction of President Bush. It coordinates strategic analyses of threats based upon intelligence from various agencies and operates out of Langley, Virginia.

In addition to all this, the FBI sends out weekly intelligence bulletins to over 1700 law enforcement agencies and 60 federal agencies. I am looking forward to hearing more about these areas during this hearing.

These impressive accomplishments notwithstanding, the FBI does face some challenges. Let me start by commending Director Mueller for taking on the Herculean task of modernizing the information technology systems at the FBI, a project which we all know of as Trilogy. It is not an easy task to update both local and wide area networks and install 30,000 new desktop computers, but you have accomplished that and I congratulate you.

I understand that you have been consulting with various outside experts seeking their advice on the Trilogy project and have received much praise for working cooperatively with them and being receptive to their recommendations. For example, I know that you actively sought out the expert advice of the National Research Council of the National Academies. Their initial report, which was released last week, made some important observations, and a subsequent updated report will be forthcoming. I was particularly impressed that some of the recommendations that they made in the initial report had already been implemented by the FBI before the report was released.

I know that you still have a very long way to go on this project and that you are still working with various experts on the Virtual Case File system as well as other aspects of Trilogy. I have every confidence that you will continue to be responsive and will do whatever it takes to get an effective IT system up and running.

On another note, I know that the FBI, like most federal agencies, is facing the challenge of finding qualified linguists. While the demand for linguists in various dialects of Arabic, Farsi, Pashto, Urdu and other Asian or Middle Eastern languages continue to be in high demand, I am heartened to hear that the FBI has added nearly 700 translators since September 2001. I am reassured that the FBI has exacting standards, that 65% of its applicants are screened out by a series of qualification tests, and that the FBI has quality control measures in place to ensure that translations are accurate and complete.

Although I recognize that the FBI needs to hire more translators to meet their growing demand, I appreciate that you have adopted an aggressive recruitment strategy, advertising in both foreign language and mainstream media, and targeting foreign language departments in American universities, military outplacement posts, and local ethnic communities. I also appreciate that you have prioritized tasks so that the most significant counterterrorism or counterintelligence assignments are done first, often within 12 hours. I look forward to hearing more on this issue.

###

Statement of Senator Patrick Leahy,
Ranking Democratic Member, Senate Judiciary Committee
FBI Oversight: Terrorism and Other Topics
May 20, 2004

Director Mueller's First 1000 Days

Good morning, Director Mueller, and welcome back to the Committee. We thank you and the Bureau's hard-working and skillful staff for all you do on behalf of the safety and security of the American people, especially during these difficult times. We know you have one of the toughest jobs in America.

If I have occasion to sound somewhat abrupt as we begin this hearing, it is because of my frustration at the circumstances under which we must now make the most of your time. For some reason, the decision has been made to schedule other business of the Committee before your testimony, and on a day with a number of floor votes and with competing obligations that some of our Majority members have this morning.

This also happened the last time you were here. We kept you waiting for hours while we held a contentious executive business meeting. We wasted your time, we wasted our other witness's time, and we squandered our own time, because by the time you had to leave, there was scarcely enough time for opening statements and one short round of questions.

These scheduling matters are not our call. In fact I had urged that your hearing be scheduled for a time certain this morning and that we resume the markup thereafter. I apologize to you and hope you will find time to join us again, soon, so that we can cover the many important matters of interest to Members of this Committee that we will not be able to get to today because of the way in which the Majority has again chosen to proceed.

Your testimony before us will never be considered as an afterthought by me or by others who share a commitment to oversight and government accountability. We need to hear from you on a myriad of issues that directly affect our legislative and oversight responsibilities. Your testimony should always be our lead agenda item when you are invited to Capitol Hill.

Difficult Issues And Constructive Criticism

Director Mueller, you know that I have been supportive of your efforts to more effectively concentrate the FBI's resources on the threats and challenges that the Nation faces today. As Chairman of the Committee at the time of your nomination, I worked hard to clear the path before you. I have done what I can since then to help you reform and refocus the Bureau. When I have had concerns, I have sometimes raised them with you privately, and I have always tried to be constructive. I very much wanted you to succeed then, and I want you to succeed now. And that is the spirit in which I will raise several difficult issues that need to be addressed during our discussion today.

Nicholas Berg's Last Weeks in Iraq

I want to turn briefly to the war in Iraq because there are so many unanswered questions regarding the case of Nicholas Berg, the American who was so brutally murdered earlier this month. In addition, we await a great deal of information from the Administration regarding the interrogation and treatment of prisoners in U.S. custody in Iraq and elsewhere.

Regarding Mr. Berg, questions have been raised about the circumstances that prevented his leaving Iraq in March, as he had planned. Mr. Berg's father claims that his son was detained illegally by the U.S. military for nearly two weeks, and would otherwise have been able to leave Iraq before the violence worsened. The FBI acknowledges that it questioned Mr. Berg repeatedly about what he was doing in Iraq, but says that the Iraqi police, not the U.S. military, held him in custody. The Iraqi police insist that they never arrested Mr. Berg and had no knowledge of the case. A coalition spokesman has promised a thorough investigation, and said that the FBI would probably have overall direction of that inquiry.

I said last week that I would try to be of assistance to Mr. Berg's family and to Senator Specter, as he does his best to help them obtain information. Director Mueller, I will ask you today about the FBI's role in the detention and interrogation of Mr. Berg, and what steps American authorities took to secure his safety and his safe departure from the war zone.

Civilian Contractors

It is clear from the Berg case that the FBI is operating in Iraq. We need more information about what FBI agents are doing there. I hope that the FBI is investigating the alleged abuse of Iraqi prisoners by civilian contractors, who, as we all know, are not subject to military courts martial.

In 2000, Congress closed a jurisdictional gap that previously existed for crimes committed by American civilians who work as employees or as contractors to the military and who are deployed with our forces oversees. Under the Military Extraterritorial Jurisdiction Act, which I worked with Senators Sessions and DeWine to enact in the 106th Congress, a contractor or subcontractor of the military can be prosecuted in Federal court if the crime of which he is

accused is a felony when committed in the United States. Two weeks ago, I asked the Assistant Attorney General for the Criminal Division whether the Department was involved in investigating the allegations against civilian contractors and was told that it was not. I asked to be kept abreast of developments and needless to say have not heard another word from him.

The Department of Defense has yet to promulgate regulations under MEJA. Curiously, it finally got around to proposing rules to implement the law on February 2, 2004, a few weeks after it began a criminal investigation into the reported abuses at the Abu Ghraib prison. But even without regulations, the law can be used. In fact, it was used last year to prosecute the spouse of an Air Force staff sergeant. She was charged in connection with the death of her husband at Incirlik Air Base in Turkey.

I have asked Chairman Hatch to hold a hearing on the reported abuse of prisoners by Americans in Iraq. Given the wide-ranging jurisdiction of the Judiciary Committee over civil liberties and prisons, the reported role of civilian contractors, and our role in enactment of the Military Extraterritorial Jurisdiction Act, we have a responsibility to act.

FBI Knowledge of Questionable Interrogation Practices

We have all seen the photos from Abu Ghraib. Red Cross observers who witnessed some of the abuse concluded that it was, in some cases, "tantamount to torture."

Torture is a crime. It is a crime under the Convention Against Torture, to which we are a party, and it is a crime under our Constitution. It is a crime whether it happens in this country or any other country. It is a crime whether it is an American soldier who is the victim or a suspected member of al Qaeda. Use of torture and other abuses of those in U.S. custody endangers our troops and our civilians overseas, and it undermines our national security and foreign policy interests abroad. But even when the authorities were warned about it, and were asked about it, and the press and human rights groups wrote about it, the Administration did next to nothing. In fact they ignored oversight inquiries, they made self-serving, reassuring statements that turned out to be false, and they continued to let it go on.

Torture is also a notoriously unreliable means of extracting information. Senator McCain has discussed this on many occasions, and I tend to trust his judgment based on his experience as a POW in a North Vietnamese prison. Senator McCain recently said, "history shows that mistreatment of prisoners and torture is not productive. ... You don't get information that's usable from people under torture because they just tell you whatever you want to hear."

A recent *New York Times* article made the same point. It told the story of one Iraqi prisoner in Abu Ghraib, who said that after 18 days of "being hooded and handcuffed naked, doused with water, threatened with rape and forced to sit in his own urine," he was "ready to confess to anything." When his interrogators asked him about Osama bin Laden, he replied, "I am Osama bin Laden. I am disguised."

According to the Army's own field manual on intelligence interrogation, "experience indicates that the use of force is not necessary to gain the cooperation of sources for interrogation. Therefore, the use of force is a poor technique, as it yields unreliable results, may damage subsequent collection efforts, and can induce the source to say whatever he thinks the interrogator wants to hear."

A recent issue of the FBI Law Enforcement Bulletin stated that felons are more likely to confess to an investigator who treats them with respect, and the interview should be a "seduction, not a showdown."

Press accounts from last week suggested that the FBI shied away from participating in or observing certain interrogations of terrorism suspects. *The New York Times* reported on May 13 that "FBI officials have advised the bureau's director, Robert S. Mueller III, that the interrogation techniques, which would be prohibited in criminal cases, could compromise their agents in future criminal cases."

For over a year I have sought answers from the Department of Justice, the FBI, the CIA and the Department of Defense regarding reported, and in some instances documented, cases of the abuse of prisoners in U.S. custody. But this was the first time I encountered a mention of the FBI's knowledge of such practices. I look forward to exploring this issue today.

FBI Reform Still Overdue

Almost 1,000 days have passed since September 11, 2001, and since you took over the helm at the FBI. This Committee and the Senate moved your nomination in record time in the summer of 2001. Since your confirmation three years ago, we have been assured that big changes are taking place at the FBI and, to be sure, we have seen some changes -- at least on paper. There are new leadership positions; offices have been reorganized; fancy new "systems" and "programs" with impressive names like the "Secure Collaborative Operational Prototype Environment (SCOPE)" and the "National Criminal Intelligence Sharing Plan" have been announced.

But in our oversight role, this Committee examines actions -- actions that often speak louder and clearer than any words or acronyms.

It has been said that if you want to truly understand something, try to change it. Out of the tragedy of September 11, we tried to understand the FBI, and we learned the institution had serious problems. And in trying to change it, we understood more about the bureaucratic culture that has made these problems so difficult to solve.

This past April, the 9/11 Commission dealt the FBI some of the worst criticism yet. The Commission found that much of the FBI does not work, and Commissioners expressed uncertainty as to how to fix it. In the months ahead, this debate will inevitably turn to whether

the FBI is the right agency for the job of handling domestic intelligence and counterterrorism. Some believe it is not -- because the FBI's foundation in criminal investigation is simply too ingrained, its culture of arrogance too entrenched, its bureaucracy too enmeshed with an administration unable to admit a mistake. I know Director Mueller feels differently.

Of course, none of us who have expressed concern about the FBI question the dedication and professionalism of its personnel. FBI agents risk their lives every day, both here at home, and, increasingly, overseas. FBI analysts and support personnel are as committed as ever. But the organization has to change. After 9/11, our trust in the FBI can no longer be blind. The American people need the FBI to be more effective than ever before.

Nearly three years later, after a lot of talk, this introspective phase seems neverending. Since you last testified in July 2003, more questions have arisen and old ones still linger.

Fighting terrorism is the Bureau's overriding concern. But we have yet to see to a successful prosecution here or abroad of a single 9/11 conspirator. Many are confused by a war in Iraq that is not directed at justice for the 9/11 victims; for that matter, a war that is not even about weapons of mass destruction, much less Osama bin Laden.

With the Madrid bombing that left nearly 200 dead, and hundreds more injured, we learned recently that an American may have been involved. Could this terrorist attack have been prevented? Did the record number of FISA wiretaps that have been in place since 2001 not provide a single hint of that terrorist plot?

The ricin scares that closed the Capitol last February have barely been addressed. There have been no charges brought in connection with the anthrax attacks in 2001. Instead we read headlines of lawsuits charging the Attorney General with inappropriate statements and FBI overreaching. Another high-profile prosecution of a terrorism ring in Detroit is also riddled with accusations of Justice Department misconduct and retaliation by the Attorney General.

The killer who mailed anthrax-laced letters to Senator Daschle and to me in October 2001 is still at large and we have done nothing to compensate those postal workers and others and their families who were killed or have suffered by exposure to that deadly poison.

Also alarming, the FBI has not solved even its most basic problem: Its information technology systems are hopelessly out of date. In this regard, the FBI is not much better off today than it was before September 11, 2001, when it was unable to do a computer search of its own investigative files to make critical links and connections. By all accounts, the Trilogy solution has been a disaster.

I know you are going to tell me that two phases of Trilogy were completed this past April. Yes, I know that all special agents of the FBI at last have their own computers and can send emails to each other. This is hardly a noteworthy accomplishment in this information age -- especially 500

to 600 million dollars later. But the fact is that the Automated Case System – the same system that was part of the equation of intelligence and law enforcement failure in 2001 – is still the primary IT tool for agents.

We have been told for years now that the Virtual Case File (VCF) would mean the end of an agency still heavily reliant on paper files. VCF's deadlines have been pushed back for months -- I am not even sure what it is now. I patiently waited, believing that VCF was what the FBI needed. So it was shocking to me, as it must have been to you, to review the May 2004 report of the National Academy of Sciences, which concludes that the VCF is not designed to, and will not, meet the FBI's counterterrorism and counterintelligence needs.

Staying on the subject of information technology, we need to make sure that the FBI has the capability of dealing with new technologies for communicating over the Internet that may not have been covered by the CALEA. Congress passed CALEA in 1994 to address the law enforcement concerns that emerging technologies such as call forwarding and mobile phones had on wiretap efforts. CALEA required telecommunications services to rewire their networks to support easy wiretapping. The FBI recently asked the FCC to extend CALEA to broadband Internet providers, but this is an issue that needs to be addressed by this Committee. I hope that Chairman Hatch agrees, and that we can work together on this. We must now grapple with the new technologies that have transformed the world since CALEA was signed into law a decade ago. Director Mueller, I am interested in your thinking on how Congress can be helpful here.

Then there's the FBI's internal disciplinary system, which has for many years gravely impacted agent morale and engendered public skepticism. The FBI's response to the Inspector General's report last fall was disappointing. I could not find a single public statement by the FBI indicating a willingness to address and take responsibility for the specific findings in the Report itself -- many of which were not positive about the FBI.

Director Mueller, last year I asked questions about Katrina Leung, the FBI confidential informant, and James Smith, her former FBI handler, who were indicted in an espionage case that implicated serious security lapses at the FBI. Senators Grassley, Specter and I asked Chairman Hatch for a hearing to examine issues raised by this case. Unfortunately, our request was refused. Last week I learned about the agent's plea to a lesser charge on the CNN website.

With key issues like the Iraqi prisoners and Trilogy up for discussion, other important topics like the PATRIOT Act may get short shrift today. That is unfortunate. As former prosecutors, you and I both know that public perception of unfairness and overreaching is nearly as detrimental to the criminal justice system as the reality of it. A law that touches upon complex issues as varied as foreign intelligence gathering, immigration, and international money laundering, among other things, could surely benefit from a closer examination. But this Administration just wants a blank check on its extension and recently came before this Committee to ask that the law be expanded further with vague language.

The courts have barely had time to grapple with legal issues implicated by its passage. And only

the government really knows what goes on in the secret FISA court. With Senator Grassley, Senator Specter, and others, I continue to press for legislative changes that would shed some light on the operations of that court, but to no avail. We are left to speculate why, for example, four FISA applications were sought in 2003 but rejected. Were there errors in agent affidavits, like those that brought about the Woods memorandum? Is there still internal confusion about the standard for probable cause? With the paucity of legal reporting obligations in PATRIOT, and the secrecy with which this Administration has decided to operate, it is doubtful you can even answer these questions for me today, Director.

In addition to FISA, I could also spend an entire session talking about the foreign translation program at the FBI, the 41,000 hours in backlogged material needing to be translated and other issues I have raised by letter and statement over the past two years. How is the monitoring of an unprecedented 1,727 new FISA wiretaps impacting critical FBI resources? How do these numbers "translate" to the Bureau's ability to obtain, understand, assess, analyze and, if necessary, act upon threat information obtained in a foreign language and from a foreign culture?

On March 2, 2004, I asked Chairman Hatch for a hearing on this singular topic but there has been no response. If I am left with time to ask only one question today, it will be: Is the Foreign Translation Program where you want it to be, right now, today, as of this moment? This service is vital to our understanding -- literally and figuratively -- of virtually every piece of intelligence information from the Middle East. Is the program working at 110 percent? If not, why not?

It has been nearly three years since Congress directed the Attorney General to prepare a comprehensive report on the FBI's translator program. I authored that reporting requirement -- and it was a requirement, not a request. I worked to include it in the USA PATRIOT Act so that Congress could better assess the needs of the FBI for specific translation services, and make sure that those needs were met. Unfortunately, this provision of the PATRIOT Act appears to have landed in the same inbox at the Department of Justice as so many of our oversight letters.

Director Mueller, we would like to see you again this session. This month, the Committee is engaged in an important debate on a bill that federalizes virtually every violent street crime imaginable. This is also a topic from which we would all benefit by your insight, particularly given your unquestioned expertise in this area. I, for one, am unaware of any input that the FBI may have had on this bill. Is the FBI ready to add to its "to-do" list, the increased investigation of street gangs, state murders, state obstruction of justice cases, carjackings, and 16- and 17-year-old defendants? And earlier this week your deputy assistant director of counterterrorism came before this Committee to urge us to expand federal criminal law to encompass "harassment" of corporations that conduct testing on animals as a top federal law enforcement priority. This suggestion comes, even as civil rights cases, health care fraud and corporate crime investigations take a back seat to the most urgent FBI priority: fighting terror.

We also want to hear from Attorney General Ashcroft. It has been nearly 15 months since his last appearance here. I never thought that the military commanders in Iraq, General Sanchez and General Abizaid, would testify in the Senate before we would see and hear from the Attorney

General of the United States. It leaves one to wonder if the cicadas appear on Capitol Hill more regularly than the Attorney General of the United States.

This hearing comes at an important time. One thousand days is an important milestone. Your job is not an easy one in the best of circumstances. You could not have known, when you took the job, that the world would change only seven days later, and that the FBI would have to change with it. To quote an old German proverb, to change and to change for the better are two different things. In these 1,000 days, has the FBI changed for the better?

Thank you for coming. We look forward to hearing from you today.

# # # # #

Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary
May 20, 2004

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to be here today to update you on the FBI's substantial progress in the counterterrorism and intelligence arenas since my last appearance before the Committee. I would also like to acknowledge that the progress the FBI has made in reforming our counterterrorism and intelligence programs is due in no small part to the enactment of the USA PATRIOT Act.

Every day, the men and women of the FBI demonstrate their determination to fulfill the great responsibility that you, and the public, have entrusted to them. As a result, the FBI has made steady progress in meeting our highest priority of preventing terrorism. The terrorist threat presents complex challenges. Terrorists move easily across international borders, use sophisticated technology to recruit, network, and communicate, and finance their operations with elaborate funding schemes. Above all, they are patient. They are methodical. They are determined to succeed.

But the FBI is equally determined to succeed. To defeat these threats, the FBI must have several critical capabilities: First, we must develop intelligence about terrorist activity and use that intelligence to disrupt their plans. Second, we must be global – we must work closely with our counterparts at home and abroad to develop and pool our collective knowledge and expertise. Third, we must use cutting-edge information technology to collect, analyze, manage, and share our information effectively. Most importantly, we must work within the framework of the Constitution, protecting our cherished civil liberties as we work to protect the American people.

Today, I would like to give you a brief overview of the steps we have taken to put these critical capabilities in place by reforming our counterterrorism and intelligence programs, as well as overhauling our information technology. Before I begin, however, I would like to acknowledge that none of our successes would have been possible without the extraordinary efforts of our partners in state and municipal law enforcement and our counterparts around the world. The Muslim, Iraqi, and Arab-American communities have also contributed a great deal to the war on terror. On behalf of the FBI, I would like to thank these communities for their assistance and for their ongoing commitment to preventing acts of terrorism. The country owes them a debt of gratitude.

PATRIOT ACT

Mr. Chairman, for over two and a half years, the PATRIOT Act has proved extraordinarily beneficial in the war on terrorism and has changed the way the FBI does business. Many of our counterterrorism successes, in fact, are the direct results of provisions included in the Act, a number of which are scheduled to "sunset" at the end of next year. I strongly believe it is vital to our national security to keep each of these provisions intact. Without them, the FBI could be forced back into pre-September 11 practices, attempting to fight the war on terrorism with one hand tied behind our backs.

Let me give you just a few examples that illustrate the importance of the PATRIOT Act to our counterterrorism efforts:

First and foremost, the PATRIOT Act – along with the revision of the Attorney General's investigative guidelines and the 2002 decision of the Foreign Intelligence Surveillance Court of Review – tore down the wall that stood between the intelligence investigators responding to terrorist threats and the criminal investigators responding to those same threats.

- Prior to September 11, an Agent investigating the intelligence side of a terrorism case was barred from discussing the case with an Agent across the hall who was working the criminal side of that same investigation. For instance, if a court-ordered criminal wiretap turned up intelligence information, the criminal investigator could not share that information with the intelligence investigator – he could not even suggest that the intelligence investigator should seek a wiretap to collect the information for himself. If the criminal investigator served a grand jury subpoena to a suspect's bank, he could not divulge any information found in those bank records to the intelligence investigator. Instead, the intelligence investigator would have to issue a National Security Letter in order to procure that same information.

- The removal of the "wall" has allowed government investigators to share information freely. Now, criminal investigative information that contains foreign intelligence or counterintelligence, including grand jury and wiretap information, can be shared with intelligence officials. This increased ability to share information has disrupted terrorist operations in their early stages -- such as the successful dismantling of the "Portland Seven" terror cell -- and has led to numerous arrests, prosecutions, and convictions in terrorism cases.

- In essence, prior to September 11th, criminal and intelligence investigators were attempting to put together a complex jigsaw puzzle at separate tables. The Patriot Act has fundamentally changed the way we do business. Today, those investigators sit at the same table and work together on one team. They share leads. They fuse information.

Instead of conducting parallel investigations, they are fully integrated into one joint investigation.

- Because of the creation of the Terrorist Threat Integration Center, and because the FBI has dramatically improved its information sharing with the CIA, the NSA, and a host of other federal, state, local and international partners, our resources are used more effectively, our investigations are conducted more efficiently, and America is immeasurably safer as a result. We cannot afford to go back to the days when Agents and prosecutors were afraid to share information.

Second, the PATRIOT Act gave federal judges the authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigations. In the past, a court could only issue a search warrant for premises within the same judicial district – yet our investigations of terrorist networks often span multiple districts. The PATRIOT Act streamlined this process, making it possible for judges in districts where activities related to terrorism may have occurred to issue search warrants applicable outside their immediate districts.

In addition, the PATRIOT Act permits similar search warrants for electronic evidence such as email. In the past, for example, if an Agent in one district needed to obtain a search warrant for a subject's email account, but the Internet service provider (ISP) was located in another district, he or she would have to contact an AUSA and Agent in the second district, brief them on the details of the investigation, and ask them to appear before a judge to obtain a search warrant – simply because the ISP was physically based in another district. Thanks to the PATRIOT Act, this frustrating and time-consuming process can be averted without reducing judicial oversight. Today, a judge anywhere in the U.S. can issue a search warrant for a subject's email, no matter where the ISP is based.

Third, the PATRIOT Act updated the law to match current technology, so that we no longer have to fight a 21st-century battle with antiquated weapons. Terrorists exploit modern technology such as the Internet and cell phones to conduct and conceal their activities. The PATRIOT Act leveled the playing field, allowing investigators to adapt to modern techniques. For example, the PATRIOT Act clarified our ability to use court-ordered pen registers and trap-and-trace devices to track Internet communications. The Act also enabled us to seek court-approved roving wiretaps, which allow investigators to conduct electronic surveillance on a particular suspect, not a particular telephone – this allows them to continuously monitor subjects without having to return to the court repeatedly for additional authorizations. This technique has long been used to investigate crimes such as drug trafficking and racketeering. In a world in which it is standard operating procedure for terrorists to rapidly change locations and switch cell phones to evade surveillance, terrorism investigators must have access to the same tools.

In a final example, the PATRIOT Act expanded our ability to pursue those who provide material support or resources to terrorist organizations. Terrorist networks rely on individuals for fund-raising, procurement of weapons and explosives, training, logistics, and recruiting. The material support statutes allow investigators to aggressively pursue and dismantle the entire terrorist network, from the financiers to those who carry out terrorist plans. By criminalizing the actions of those who provide, channel, or direct resources to terrorists, the material support statutes provide an effective tool to intervene at the earliest possible stage of terrorist planning. This allows the FBI to arrest terrorists and their supporters before their deadly plans can be carried out.

For instance, the FBI investigated a case in Charlotte, North Carolina, in which a group of Lebanese nationals purchased mass quantities of cigarettes in North Carolina and shipped them to Michigan for resale. Their scheme was highly profitable due to the cigarette tax disparity between the two states. The proceeds of their smuggling were used to fund Hezbollah affiliates and operatives in Lebanon. Similarly, the FBI investigated a case in San Diego in which subjects allegedly negotiated with undercover law enforcement officials the sale of heroin and hashish in exchange for Stinger anti-aircraft missiles, which they indicated were to be sold to Al Qaida. In both cases, the material support provisions allowed prosecutors to charge the subjects and secure guilty pleas and convictions.

Mr. Chairman and Members of the Committee, the importance of the PATRIOT Act as a valuable tool in the war against terrorism cannot be overstated. It is critical to our present and future success. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect innocent lives, while at the same time protecting civil liberties.

COUNTERTERRORISM AND INTELLIGENCE PROGRAM REFORMS

Let me turn for a few moments to the progress the FBI has made in strengthening and reforming its counterterrorism and intelligence programs to support its number one goal of terrorism prevention. Today, the FBI is taking full advantage of our dual role as both a law enforcement and an intelligence agency. Let me give you just a few examples of the progress we have made:

- We have more than doubled the number of counterterrorism Agents, intelligence analysts, and linguists.

- We expanded the Terrorism Financing Operations Section, which is dedicated to identifying, tracking, and cutting off terrorist funds.

- We are active participants in the Terrorist Threat Integration Center and the Terrorist Screening Center, which provides a new line of defense against terrorism by making information about known or suspected terrorists available to federal, state, and local law enforcement.

- We have worked hard to break down the walls that have sometimes hampered our coordination with our partners in federal, state and local law enforcement. Today, the FBI and CIA are integrated at virtually every level of our operations. This cooperation will be further enhanced when our Counterterrorism Division co-locates with the CIA's Counter Terrorist Center and the multi-agency Terrorist Threat Integration Center.

- We expanded the number of Joint Terrorism Task Forces (JTTF) from 34 to 84 nationwide.

- We created and refined new information sharing systems, such as the National Alert System, that electronically link us with our domestic partners.

- We have sent approximately 275 FBI executives to the Kellogg School of Management at the University of Chicago to receive training on executive leadership and strategic change.

Recognizing that a strong, enterprise-wide intelligence program is critical to our success across all investigations, we have worked relentlessly to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the FBI:

- We stood up the Office of Intelligence, under the direction of a new Executive Assistant Director for Intelligence. The Office of Intelligence sets unified standards, policies, and training for analysts, who examine intelligence and ensure it is shared with our law enforcement and intelligence partners. The Office of Intelligence has already provided over 2,600 intelligence reports and other documents for the President and members of the Intelligence Community.

- We established a formal analyst training program. We are accelerating the hiring and training of analytical personnel, and developing career paths for analysts that are commensurate with their importance to the mission of the FBI.

- We developed and are in the process of executing Concepts of Operations governing all aspects of the intelligence process – from the identification of intelligence requirements

to the methodology for intelligence assessment to the drafting and formatting of intelligence products.

- We established a Requirements and Collection Management Unit to identify intelligence gaps and develop collection strategies to fill those gaps.

- We established Reports Officers positions and Field Intelligence Groups in the field offices, whose members review investigative information – not only for use in investigations in that field office – but to disseminate it throughout the FBI and among our law enforcement and Intelligence Community partners.

With these changes in place, the Intelligence Program is established and growing. We are now turning to the last structural step in our effort to build an intelligence capacity. In March, I authorized new procedures governing the recruitment, training, career paths and evaluation of our Special Agents – all of which are focused on developing intelligence expertise among our agent population.

The most far-reaching of these changes will be the new agent career path, which will guarantee that agents get experience in intelligence investigations and with intelligence processes. Under this plan, new agents will spend an initial period familiarizing themselves with all aspects of the Bureau, including intelligence collection and analysis, and then go on to specialize in counterterrorism, intelligence or another operational program. A central part of this initiative will be an Intelligence Officer Certification program that will be available to both analysts and agents. That program will be modeled after – and have the same training and experience requirements as – the existing programs in the Intelligence Community.

INFORMATION TECHNOLOGY IMPROVEMENTS

All the progress the FBI has made on all investigative fronts rests upon a strong foundation of information technology. Over the past two and a half years, the FBI has made tremendous efforts to overhaul our information technology, and we have made significant progress.

- Over 1,000 counterterrorism and counterintelligence FBI Headquarters employees have been provided with access to Top Secret/Sensitive Compartmented Information (TS/SCI) information at their desks.
- We implemented the Wide Area Network and the Enterprise Operations Center on schedule in March 2003.

- We improved data warehousing technology to dramatically reduce stove-piping and cut down on man-hours that used to be devoted to manual searches.

- The Full Site Capability deployment began in February of this year, and was completed on April 29th. Altogether, nearly 30,000 workstations have been converted to the new Trilogy baseline software and new email system.

- We now have a permanent Chief Information Officer and Chief Technology Officer, who oversee the development and management of all IT projects and systems throughout the FBI. It is important to keep in mind that Trilogy is not the FBI's sole IT system – the FBI has over 200 IT systems, all of which must be maintained, enhanced when necessary, and certified and accredited for security.

As you know, during the past year we have encountered some setbacks regarding the deployment of Trilogy's Full Site Capability (FSC) and the Virtual Case File. Our goal is to deliver Virtual Case File capabilities by the end of this year. You are aware that last week, the National Research Council of the National Academies (NRC) released a report reviewing the Trilogy IT Modernization program. The FBI commissioned this review as part of our ongoing efforts to improve our capabilities to assemble, analyze and disseminate investigative and operational data both internally and externally with other intelligence and law enforcement agencies.

Many of the NRC's recommendations have already been implemented or are a work in progress. The FBI has repeatedly sought outside evaluation and advice throughout its IT modernization efforts and will continue to do so. The NRC report specifically noted that the counterterrorism mission requires extensive information sharing, and recommended that the FBI involve other agencies in its modernization program. We will continue to work closely with other Department of Justice Agencies and members of the Homeland Security and Intelligence Communities to ensure the FBI has the right technology to support information sharing and other mission requirements.

CONCLUSION

With our counterterrorism, intelligence, and information technology initiatives firmly in place, the FBI is moving steadily forward, always looking for ways to evolve and improve so that we remain a step ahead of our enemies. We are looking at ways to assess and adjust our resource needs based on threats, in order to ensure that we have the personnel and resources to meet and defeat all threats.

Mr. Chairman, I would like to commend the men and women of the FBI for their hard work and dedication – dedication both to defeating terrorism and to upholding the Constitution. They have embraced and implemented the counterterrorism and intelligence reforms I have outlined for you today and they are committed to upholding their duty to protect the citizens of the United States.

Mr. Chairman, thank you again for the Committee's support of the FBI and for the opportunity to be here this morning.

I would be happy to answer any questions you might have.

###

New York's Senator

CHARLES E. SCHUMER

313 Hart Senate Office Building • Washington, DC 20510
Phone: (202)224-7433 • Fax: (202)228-1218

FOR IMMEDIATE RELEASE
May 20, 2004

CONTACT: Brent Colburn
(202) 224-7433

SCHUMER: SECOND CORRECTIONS OFFICIAL WITH CHECKERED RECORD PUT IN POWER POSITION AT IRAQI PRISONS

John Armstrong, Forced Out as Head of Connecticut Corrections for Questionable Record Involving Mistreatment of Inmates, Now Serves as Deputy Director of Operations for Iraqi Prisons

Armstrong Joins Lane McCotter as Another Prison Official in Iraq with Troubling Record of Defending Inmate Abuse

Schumer Demands DOJ Investigation of Crimes by Civilian Contractors

U.S. Senator Charles E. Schumer today revealed that a second prison official in Iraq has a troubling history of defending prisoner abuse and called on Attorney General John Ashcroft to immediately initiate an investigation of all crimes committed by civilian contractors in the Iraqi prison system.

Schumer discovered that John Armstrong, was forced from his post as the head of Connecticut's corrections department for defending abuses of prisoners but now serves in a high-ranking management position overseeing the Iraqi prison system. While running Connecticut's prison system, Armstrong made a practice of shipping even low-level offenders to a supermax facility in Virginia which was notorious for its use of excessive force - ranging from unjustified use of stun guns shooting 50,000 volts through prisoners to locking inmates in five-point restraints for such lengthy periods that they were routinely forced to defecate on themselves.

Furthermore, Armstrong resigned under a cloud of credible allegations that he tolerated and personally engaged in the sexual harassment of female employees under his command.

Despite this checkered record, Armstrong was tapped to serve as the deputy director of operations for the Iraqi prison system. The new revelations about Armstrong come a week after Schumer reported that Ashcroft appointed another former prison official, Lane McCotter, who had a similarly disturbing history of defending inmate abuses, to be one of four individuals sent by the Department of Justice to redevelop Iraq's prison system. McCotter subsequently served at Abu Ghraib where, among his responsibilities, was designing

training programs for guards.

"One official with a history of prisoner abuse raises an eyebrow, but two means we have a problem. Why we would send officials with such disturbing records to handle such a sensitive mission is beyond me and it demands explanation," Schumer said.

In a letter to Ashcroft, Schumer called for the Department of Justice to immediately undertake a complete investigation of the role civilian contractors have played in crimes against Iraqi prisoners and prosecute those responsible to the full extent of the law.

"If DOJ does not investigate and prosecute the civilians who may have committed crimes, no one will," Schumer wrote, adding, "We have an obligation to ensure that all those responsible are brought to justice and we have duty to guarantee that a handful of privates do not take the fall if they were directed by others."

Schumer expressed concern that the Department of Defense is planning to investigate crimes by civilian contractors and pass its findings along to the Department of Justice. "The DOD investigators know how to go after military crimes, but civilian crimes to be prosecuted in civilian courts are a whole different ball of wax. We need professional prosecutors and criminal investigators on the job and we need them now," Schumer said.

Schumer noted that Ashcroft has not responded to a series of questions Schumer sent him last week regarding the appointment of McCotter who was ousted from his job as the head of Utah's corrections systems when a schizophrenic inmate died after being strapped naked to a chair for 16 hours and McCotter defended the practice. McCotter also was an executive with a private prison company under investigation for abuses of inmates' civil rights and denying them access to medical care when Ashcroft selected him for the Iraq prison mission.

"We're sending abusers of prisoners' rights to Iraq and putting them in charge of prisons where we now learn abuses are occurring. We need to know why this is happening and what's being done about it," Schumer said.

Schumer's letters to Ashcroft are attached.

###

CHARLES E. SCHUMER
NEW YORK

COMMITTEES:
BANKING
JUDICIARY
RULES

United States Senate

WASHINGTON, DC 20510

May 20, 2004

The Honorable John Ashcroft
Attorney General
U.S. Department of Justice
950 Pennyslvania Avenue N.W.
Washington, DC 20530-0001

Dear Attorney General Ashcroft:

I write to express my profound concern that the Department of Justice is not aggressively investigating civilian contractors for their roles in prison abuses in Iraq.

In light of new evidence I have uncovered showing that another civilian contractor overseeing the redevelopment of Iraq's prison system has a checkered record when it comes to prisoners rights, I ask that you immediately undertake a full investigation of the role civilian contractors have played in all crimes against Iraqi prisoners and prosecute those responsible to the full extent of the law. If DOJ does not investigate and prosecute the civilians who may have committed crimes, no one will.

Last week I wrote you about a civilian contractor working under a contract with the Department of Justice. Lane McCotter, a former corrections official with a history of support for abusive treatment of inmates and disregard for their basic rights, was chosen by you to assist in redeveloping Iraq's prison system and ultimately was posted at Abu Ghraib. I am still awaiting your answers to my questions regarding how, given his background, Mr. McCotter could have been picked for such a sensitive role and whether the Department is investigating any part he may have played in the Abu Ghraib crimes.

Now there are questions about another civilian contractor overseeing the redevelopment of Iraq's prison system who has a checkered record when it comes to prisoners rights.

Like Mr. McCotter, John Armstrong, was forced from his post as the head of a state corrections department for defending abuses of prisoners. While running Connecticut's prison system, Mr. Armstrong made a practice of shipping even low-level offenders to a supermax facility in Virginia which was notorious for its use of excessive force - ranging from unjustified use of stun guns shooting 50,000 volts through prisoners to locking inmates in five-point restraints for such lengthy periods that they were routinely forced to defecate on themselves. Furthermore, Mr. Armstrong resigned under a cloud of credible allegations that he tolerated and personally engaged in the sexual harassment of female employees under his command.

Mr. Armstrong subsequently was appointed by the State Department to be the deputy director of operations for the Iraqi prison system both before and during the time frame during which abuses

occurred.

The Department of Justice has indicated that it is investigating the deaths of two Iraqi prisoners, but you have said nothing about your intent to investigate and prosecute all civilian contractors who may have committed felony crimes in the Iraqi prison system. We have an obligation to ensure that all those responsible are brought to justice and we have duty to guarantee that a handful of privates do not take the fall if they were directed by others.

I am deeply concerned that civilian contractors, who are not subject to the military justice system, are closely scrutinized for their roles in the Iraqi prison abuses. All those responsible for crimes must be prosecuted and punished to the full extent of the law.

I look forward to your prompt response to these questions and the questions I posed in my letter of last week.

Sincerely,

Charles Schumer

Charles E. Schumer
United States Senator

CHARLES E. SCHUMER
NEW YORK

COMMITTEES:
BANKING
JUDICIARY
RULES

United States Senate

WASHINGTON, DC 20510

May 13, 2004

The Honorable John Ashcroft
Attorney General
U.S. Department of Justice
950 Pennyslvania Avenue N.W.
Washington, DC 20530-0001

Dear Attorney General Ashcroft:

It has come to my attention that an individual with ties to prisoner mistreatment in Utah in 1997, Lane McCotter, was selected by you to be part of the team redeveloping the criminal justice system in Iraq. Given Mr. McCotter's troubling history in the criminal justice system, I have a number of questions regarding why Mr. McCotter was chosen for such a sensitive role.

Mr. McCotter was the director of Utah's Department of Corrections when Michael Valent, a 29-year old schizophrenic inmate, died after being strapped naked to a chair for 16 hours. The treatment of Mr. Valent was described by a number of critics as "torture". Nonetheless, Mr. McCotter defended what was done to Mr. Valent, saying, "You have to have a way to deal with violent inmates."

As a result of what happened to Mr. Valent and Mr. McCotter's refusal to deal with the situation appropriately, Mr. McCotter was forced to resign his post at the Department of Corrections. He subsequently became an executive at a private prison company which reportedly was under Department of Justice investigation for failing to provide safe conditions and adequate medical care for prisoners at a Santa Fe prison when you selected him to be part of the Iraq criminal justice team.

According to press reports Mr. McCotter was one of four civilian advisors charged with the rebuilding of Iraq's prison system, including Abu Ghraib.

Like all Americans, I am disturbed by what happened at Abu Ghraib and I believe it is essential to get out all the facts as to what happened, how it happened, and why it happened. Mr. McCotter's checkered past and his selection for this important position raise a number of serious questions concerning the role of civilian advisors and contractors in the Iraqi prison system and of the government's selection process for and oversight of these individuals.

Why did you appoint Mr. McCotter, who had such a troubling history, to work on criminal justice reform in Iraq?

What was the formal selection process for civilian advisors selected by DOJ for work in Iraq? What level, if any, of formal background checks took place?

What safeguards did McCotter and others planning for the Iraqi corrections facilities put in place to stop potential abuse? Were they involved in designing the chain of command that so obviously failed both the United States and its Iraqi charges?

What role did McCotter and other officials play in the designing and implementation of training programs for Iraqi nationals and/or U.S. personal stationed as guards at Iraqi prisons?

Did these civilian advisors recommend or play a part in the decisions that lead to the use of private contractors in prisoner interrogations in Abu Ghraib?

Is the Department of Justice investigating Lane McCotter and other civilians for their role in the Abu Ghraib abuses?

Is the Department of Justice investigating the roles of other civilian contractors in training guards at Abu Ghraib? If so, when were those investigations initiated and what is their status? If not, why not?

I look forward to your prompt responses to these important questions.

Sincerely,

Charles Schumer

Charles E. Schumer
United States Senator