

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

May 16, 2012

Serial No. J-112-76

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

88-111 PDF

WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

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

KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa	3
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	42

WITNESSES

Witness List	41
Mueller, Robert S. III, Director Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC	5
prepared statement	44

QUESTIONS

Questions submitted by Senators Patrick Leahy, Charles Schumer, Chuck Grassley, and Lindsey Graham for Hon. Robert S. Mueller III	57
---	----

ANSWERS

Responses of Robert S. Mueller III, to questions submitted by Senators Leahy, Schumer, Grassley, and Graham	64
---	----

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois, March 27, 2012, letter	78
Mueller, Robert S. III, Director Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC., April 17, 2012, letter	81
Federal Bureau of Investigation, Counterterrorism Training Material Review .	83

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

WEDNESDAY, MAY 16, 2012

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 10:06 a.m., in Room SD-226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Kohl, Feinstein, Schumer, Durbin, Whitehouse, Klobuchar, Coons, Blumenthal, Grassley, Hatch, Kyl, Graham, and Lee.

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

Chairman LEAHY. These photographers are all good people, I have been told by my son-in-law, who used to work with them. Of course, I have a certain amount of jealousy because they have the job that I really want to have, except that they are a lot better at it than I would be. So I had to take the Senate as a second choice.

Senator Grassley, Senator Hatch, Senator Klobuchar, and Senator Coons are here, and we can begin.

It is appropriate that we welcome Director Robert Mueller of the Federal Bureau of Investigation back to the Committee during National Police Week. He and I were at the National Peace Officers Memorial Service with President Obama at the Capitol yesterday, as were others. And one of the things we talked about before, several of us did, is that every year we are losing too many fine law enforcement officers in the line of duty. It is a matter that is of great concern to me. It would be one thing if they were all being targeted by a particular organization. That does not seem to be the thing, that these are disconnected and happening in all parts of the country. But we are losing far too many police officers.

I know Director Mueller is keenly aware of their sacrifice and is focused on how best to protect those people who protect us. And I do thank him and the hard-working men and women of the FBI who work every day to keep us safe, just as I make it a point to thank the police officers here on Capitol Hill who keep us safe. But I worry about their safety, too.

Now, in the years since September 11th, the FBI has played an increasingly important role in our Nation's counterterrorism and intelligence-gathering efforts. Together with prosecutors, other law enforcement partners, and the intelligence community, the FBI has

helped obtain hundreds of terrorism convictions in our federal courts.

Earlier this month, for example, a federal jury in New York handed down a guilty verdict in one of the most serious terrorism plots since 9/11, which involved plans to carry out suicide bombings in the New York subway in 2009. I might say, contrary to the predictions of some, this major terrorism trial proceeded without a hitch in a federal court in the heart of New York City. There was hardly any disruption of the lives of New Yorkers who live and work near the courthouse, and they were convicted.

The defendant was convicted without the need for mandatory military custody or interrogation, certainly without the need for indefinite detention at Guantanamo Bay or elsewhere. He is going to be sentenced later this year. He faces life imprisonment. But it is only the latest example—and there are many, many, many of them—of federal law enforcement, prosecutors, and criminal courts successfully investigating and trying terrorism cases. In recent years, the Christmas Day bomber and the Times Square bomber were convicted and sentenced to life imprisonment after the FBI used its expertise and experience to obtain statements after giving Miranda warnings, and they did all that without resorting to torture, and not only got a great deal of information, some of which we cannot go into in an open session, but they also got convictions.

In contrast, the military commissions proceedings against the 9/11 plotters are just beginning at Guantanamo Bay. And we know there is going to be lengthy litigation concerning the torture and mistreatment of certain defendants. The trial itself will not start until sometime next year, unlike those trials that have already been completed, and people are being sentenced. Moreover, as Director Mueller pointed out last year during the debate over the defense authorization bill, mandating military custody in these situations merely hampers the FBI's ability to react swiftly and flexibly in gathering intelligence and evidence. That is one of the reasons why I have joined Senator Mark Udall in cosponsoring the *Due Process and Military Detention Amendments Act*, which would repeal that mandatory military detention requirement.

In the coming months, I also look forward to speaking with the Director about the administration's request for reauthorization of FISA. I certainly appreciate the importance of providing the intelligence community with appropriate surveillance tools to help protect our country against terrorist threats. But we have to be sure that we are conducting sufficient oversight to ensure that we protect the privacy rights and civil liberties of law-abiding Americans. That is what I tried to do when we reauthorized certain provisions of the *USA PATRIOT Act*, and I am disappointed that common-sense, bipartisan improvements were ultimately not enacted. As Congress considers the administration's request to reauthorize the *FISA Amendments Act*, I will look at whether we should strengthen accountability or privacy or liberty protections in the various parts of it.

Now, while faced with daunting national security challenges, Director Mueller has also ensured that the FBI has maintained its historic focus on fighting crime. At a time of economic crisis and shrinking State and local law enforcement budgets, many expected

violent crime to skyrocket. Instead, crime rates across the country have continued to decline. Along with the commitment of the President and the Congress to continued federal assistance to State and local law enforcement, the dedicated service of FBI agents throughout the country has played an important role in helping to keep these crime rates low and keep Americans safe.

The FBI and the Justice Department have worked hand in hand with us to make great strides toward more effective fraud prevention and enforcement. In the last Congress, I worked hard with both Republican and Democratic Senators to craft and pass the *Fraud Enforcement and Recovery Act*, the most expansive anti-fraud legislation actually in more than a decade. We enacted important anti-fraud provisions as well as part of both the *Affordable Care Act* and Wall Street reform legislation. And I must say, Director, I am pleased to see that the FBI has greatly increased the number of agents investigating fraud. There is not only the advantage of recovering money, but it also has to have a great deterrent effect. These new agents and laws have led to record fraud recoveries and increased fraud arrests and convictions.

I commend the FBI for also continuing to combat corruption. We should pass common-sense, bipartisan legislation like the *Fighting Fraud to Protect Taxpayers Act* and the *Public Corruption Prosecution Improvements Act* to give you more tools to fight this scourge.

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

So, Director, while my voice is still working with all the pollens in here, I will yield to Senator Grassley.

**STATEMENT OF HON. CHUCK GRASSLEY, A U.S. SENATOR
FROM THE STATE OF IOWA**

Senator GRASSLEY. Chairman Leahy, thank you. Thank you, Director Mueller, for coming.

The Chairman paid tribute to Police Week, so I will not repeat those words, but I certainly agree with everything that the Chairman said.

It has been six months since our last hearing. On a housekeeping matter, the FBI has been improving response time to our requests for information, but there is still too long of a wait for some written responses. And yesterday afternoon, we received some answers to questions for the record from six months ago when the Director testified.

I want to know what efforts the FBI has undertaken to investigate the serious and grave national security leak surrounding the recently revealed operation in Yemen. National security leaks have, unfortunately, become the norm with far too much sensitive information being leaked about ongoing operations. They are dangerous and have grave consequences. They threaten sensitive sources and methods and endanger life and complicate relationships with our allies. So I hope to hear from the Director what the FBI is doing to investigate that leak and bring people to justice.

Next, there are a couple pressing national security policy matters that we need to address in the Senate. As the Director pointed out in written testimony, the *FISA Amendments Act* expires at the end of the year. This critical national security tool needs to be reauthor-

ized, and I would like to hear from the Director about the urgency in pushing that reauthorization.

The Communications Assistance for Law Enforcement Act is important. We have been waiting patiently for the administration to put forth a proposal with necessary fixes to ensure that the going-dark problem is addressed. This needs to be addressed in a correct manner. There is a lot of misinformation on this issue floating around, and the sooner we have a proposal, the sooner we can work to dispel those misconceptions.

For starters, it is not a plan for the Government to take over the Internet or other mediums. It involves compliance with valid, lawfully issued court orders. Simply, it is about ensuring that when a court issues an order, law enforcement can obtain the information the court authorizes. I want the Director to give us the status on this proposal and when the administration plans to send something up to the Hill.

Another critical national security issue to address is cybersecurity. The House has passed four separate bills in this area. There are a number of other bills pending before the Senate. While a lot of attention has been focused on differences between these bills, the proposals do have much in common. All the proposals recognize the need to strengthen the Nation's cybersecurity defenses. Where they differ is how to do it, so I hope the Director can fill us in on concerns that I have with proposals that create new bureaucracies to deal with cybersecurity. I will ask the Director about the danger of compartmentalizing cybersecurity-related threat information and whether such efforts would lead to reconstituting the wall between national security and criminal matters.

Aside from national security, the FBI continues to handle a significant caseload of traditional criminal matters. One matter of concern is a recent report in the *Washington Post* about a number of cases where individuals may have been convicted based upon faulty FBI crime lab reports. This issue dates back to the 1990s when I conducted oversight work on the FBI crime lab, when they spent \$1 million to settle with a whistleblower, build a new lab. I am interested in—what is concerning me is that the recent reports indicate that the Justice Department's review of these cases may have been incomplete and that defendants in cases may not have been notified about problems. It is troubling. However, what is even more troubling is that it appears the Justice Department never made public the findings of the report, nor does it appear these findings were reported to Congress.

Given the high-profile problems with disclosing exculpatory evidence and serious misconduct by FBI and DOJ officials in the prosecution of Senator Stevens, this report has raised a number of questions. I want to hear from the Director what he has done as part of this review and what is being done to address these cases.

Time permitting, there are a number of other topics. I remain concerned that whistleblowers at the FBI face retaliation and delays in clearing their names. Just yesterday we received written responses from the Director's last appearance where he addressed the long-running whistleblower cases of Turner and Kobus. These cases have languished at the Justice Department for many years despite clear findings of retaliation for protected whistleblowing,

nearly 10 years in the Turner case and four years for Kobus. So, obviously, I am disappointed in the Director's written answers. They fail to answer the basic question about when these matters will come to an end and are chock full of legalese. They do nothing to bring closure to these matters, which I consider a black eye for the Bureau. In fact, one response states that the Director cannot answer because of ongoing litigation. So, note, the litigation is only ongoing because the FBI continues to appeal the case. At some point the FBI needs to own up to the retaliation and end these cases. That is something within the Director's power, something he could and should do immediately.

Finally, I want to thank the Director for his candor in answering one of my written questions about the FBI's attempt to overclassify a memorandum provided to us. In a rare admission of fault, the written questions noted that the FBI erroneously stamped a memo to the Congress as "sensitive security information" under the Code of Federal Regulations. At first glance, this stamp appeared to limit disclosure of the memo; however, a closer look revealed the FBI was attempting to classify the memo using the authority reserved for the Administrator of TSA and Secretary of Transportation. While we in Congress understand the need to appropriately classify certain information, this was an example of the overreach that has made us cynical about overclassification of materials, and so I am very happy that the FBI owned up to this erroneous classification but worried that it may signal a greater problem.

I look forward to addressing these topics. Thank you very much. Chairman LEAHY. Thank you.

Director Mueller, please go ahead, sir.

STATEMENT OF THE HON. ROBERT S. MUELLER III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. MUELLER. Good morning, and thank you, Chairman Leahy and Ranking Member Grassley and Members of the Committee. I want to thank you for the opportunity to appear before the Committee today and most particularly thank you for your continued support of the men and women of the FBI.

As you have pointed out, the Bureau has undergone unprecedented change in recent years. Since the attacks of September 11th, we have refocused our efforts to address and prevent emerging terrorist threats, which are more diverse than they were 10 years ago. And we also face increasingly complex threats to our Nation's cybersecurity as nation state actors, organized criminal groups, and hackers for hire are stealing trade secrets and valuable research from America's colleges, America's companies, and our government agencies. And, of course, we must also combat investment fraud, health care fraud, and mortgage fraud that have undermined the world's financial system and victimized investors, homeowners, and taxpayers.

And while crime may be down nationwide, as you pointed out, Mr. Chairman, gang violence still plagues far too many neighborhoods. And to combat these threats, we in the Bureau are relying on our law enforcement and private sector partners more than ever. And throughout these efforts, the FBI remains firmly com-

mitted to carrying out our mission while protecting the civil liberties of the citizens we serve.

Let me begin with the threat from terrorism, which does remain and still remains our top priority. Al Qaeda is decentralized, but the group is committed to high-profile attacks against the West, as we confirmed from the documents seized from Osama bin Laden a year ago. Meanwhile, Al Qaeda affiliates, especially Al Qaeda in the Arabian Peninsula, represent the top counterterrorism threat to the Nation. AQAP has attempted several attacks on the United States in 2009 and 2010, and we are currently exploiting an IED seized overseas, which is similar to explosive devices used by AQAP in the past.

We also remain concerned about the threat from homegrown violent extremists. These individuals have no typical profile; their experiences and motives are often distinct, which makes them difficult to find and difficult to stop.

Let me turn next to counterintelligence. We still confront traditional espionage. Today's spies are also students, researchers, business people, or operators of "front companies." They seek not only state secrets but also trade secrets, intellectual property, and insider information from government, businesses, and American universities.

We are also seeing a growing "insider threat"—that is, when employees use their legitimate access to steal secrets for the benefit of another company or country. And, of course, the counterintelligence threat is now merging with the cyber threat. Today so much sensitive data is stored on computer networks, our adversaries often find it as effective, or even more effective, to steal secrets through cyber intrusions.

We in the FBI have built up a substantial expertise to address the cyber threat, both here at home and abroad. We have cyber squads in each of our 56 field offices, with more than 1,000 specially trained agents, analysts, and forensic specialists. And we have 63 legal attache offices that cover the globe to also assist in addressing this threat.

And, finally, the National Cyber Investigative Joint Task Force brings together 20 law enforcement, military, and intelligence agencies to stop current and predict future cyber attacks.

Next, let me address our efforts to combat financial crimes. The FBI and its partners continue to focus on the financial executives who have committed securities and other frauds. From 2009 to 2011, there have been more than 254 executives charged with corporate fraud. And last year alone, FBI investigations led to more than 1,100 convictions for mortgage fraud. In addition, over the past four years, we have nearly tripled the number of special agents investigating mortgage fraud and other white-collar frauds.

Among them is health care fraud. Health care spending currently makes up about 18 percent of our Nation's total economy, which presents an attractive target to criminals, so much so that we lose tens of billions of dollars each year to health care fraud.

As announced two weeks ago, the FBI, HHS, and the Justice Department continue to bring a record number of cases involving hundreds of millions of dollars in Medicare fraud. Indeed, since their inception in March 2007, Medicare Fraud Strike Force operations

in nine locations have charged more than 1,300 defendants who collectively have falsely billed the Medicare program for more than \$4 billion.

And crime on our streets remains as much of a threat to our overall security as terrorism, espionage, or cyber crime. And the most recent Uniform Crime Report does indicate violent crime continues to fall. But as we all know, this does not represent every community. For some cities and towns across the Nation, violent crime—including gang activity—continues to pose a real problem.

We also continue to confront organized crime. Today's organized crime operates multinational, multibillion-dollar schemes, everything from human trafficking to health care fraud, and from computer intrusions to intellectual property theft.

The FBI remains vigilant in its efforts to keep children safe and to find and stop child predators. Through our Child Abduction Rapid Deployment Teams, the Innocence Lost National Initiative, our Office of Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to make the world a safer place for our children.

Chairman Leahy and Ranking Member Grassley, I thank you for this opportunity to discuss the FBI's priorities, and the transformation the FBI has achieved over the past 10 years would not have been possible without your support. I would be happy to answer any questions that you might have.

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

Chairman LEAHY. Director, before we came in here, you and I discussed the question of forensics, and as you know, the *Washington Post* recently reported that a review of potential errors in hair and fiber analysis by FBI forensics experts revealed hundreds of mistakes in the 1980s and the 1990s, but that many of these mistakes were not disclosed to the people or their defense attorneys. *The Post* reported the review was very narrow and the evidence in the cases were not retested despite questions about techniques of the lab personnel.

Now, we have had a lot of attention in this Committee over the years, from both parties, about this. Your predecessor said these problems have been corrected, but what actions are being taken? Do you have a way to ensure that all questionable evidence is retested? Are there ways of making sure that notifications are made so that nobody remains in jail based on faulty evidence?

Mr. MUELLER. Mr. Chairman, there was a review done previously back—it culminated in 2004, which covered the lab that was headed by the Justice Department and, of course, we participated and cooperated in that review. Of the 13 examiners that were the subject of that review, only one was a hair and fiber analyst. And upon indications that some of those examiners who examined particular hair may have overstated the import of their examinations, the Justice Department, with ourselves contributing, is going back to look at what universe of persons may have been covered by these examiners, which cases may have had occasion where the examiners testified and did overstate the import of their examinations, and then to do whatever notifications are appropriate given that review.

At this point in time, we are not certain exactly what the universe will be, but we are working to determine that universe and make certain that we go back and identify those cases that need a further review.

The only other thing I would add is that in 1996—prior to 1996, we did not have DNA, but in 1996, we developed the mitochondrial DNA examination, which thereafter was done in conjunction with any hair and fiber examination that we had conducted.

Chairman LEAHY. It is not just the DNA, and I realize we have got new—new techniques come up all the time. I just wanted to make sure that we are doing it the best possible way because, whether it is federal prosecutors or State prosecutors, if they are relying on something from the FBI in testimony, and the courts are, we do not want to come back later on and have to say, wait a minute, this just did not work, because that is going to put in doubt prosecutions and everything else everywhere else.

So I introduced the *Criminal Justice and Forensic Science Reform Act*. This would be for a nationwide forensics reform act, including research and standards. Would that be something that might help?

Mr. MUELLER. I know that there is discussion about standardization of forensics. We have some substantial role in that now, and my expectation is whatever the administration comes out with—and I know it is looking at certain proposals. My expectation is we would continue to play a substantial role in contributing to the standards when it comes to forensics work.

Chairman LEAHY. I am sure you agree with me that, when the government has experts testify, that testimony, especially on things of a scientific nature, is the best possible.

Mr. MUELLER. Absolutely.

Chairman LEAHY. The questions of eyewitnesses and things like that, that is always subjective. But there are certain things that should be objective, and we should not have to go back afterward and say did that really work that way. I am sure you agree with that.

Mr. MUELLER. I do agree with that, and to the extent that new forensics testing such as DNA when it comes on is far more specific and accurate, we immediately adopt it. In this particular case, we need to go back and look at the universe of cases that predated the use of the DNA and determine whether there are additional notifications that need to be made.

Chairman LEAHY. Please keep this Committee posted as you go through that review.

Mr. MUELLER. Yes, sir.

Chairman LEAHY. You and I talked yesterday before the National Peace Officers Memorial Service about the number of police officers who have been killed: nationwide, 122 in 2009, 154 in 2010, 163 in 2011. This is a very troubling trend. I continue to work on the Bulletproof Vest Grant Program. I have been told by police departments all over the country that that has saved a lot of lives. I am hopeful that this Committee will reauthorize it tomorrow.

I also understand that domestic violence situations are posing special risks to officers. We voted to reauthorize the *Violence*

Against Women Act here in the Senate. The House is now looking at it.

Can you think of things that we could be doing here that might help?

Mr. MUELLER. Let me just add to the things that are being done two additional ones.

Chairman LEAHY. I assume you agree with the——

Mr. MUELLER. Absolutely.

Chairman LEAHY. With the Bulletproof Vest Program.

Mr. MUELLER. Absolutely. The Bulletproof Vest Program has saved innumerable lives, and while there was some discussion early on about making officers wear them, I think that discussion is at an end, given the benefits that everybody sees from the use of those vests.

Two additional things that we are undertaking: We have changed our new firearms training for our own agents to reflect that many of the confrontations now are a lot closer than perhaps they were in the past, and often State and local law enforcement follow our lead when it comes to firearms practices. Second, we have what we call a Violent Offender Alert System with our NCIC. When an agent or an officer stops somebody, when they look to determine their history, there will be an indication that that individual, that suspect or that person that they have detained, has a violent history. And so that will put the detaining officer or agent on alert that this is something special that you have to be aware of.

Chairman LEAHY. I will accept your invitation to come down and see the new firearms training.

Mr. MUELLER. Yes.

Chairman LEAHY. And, last, you have testified before about the need for law enforcement to keep pace with developments in communication technology and so on. We have CALEA, the *Communications Assistance Law Enforcement Act*, that I drafted and helped to enact back in the 1990s. Some have suggested updating it. There have been press reports that the FBI is seeking to expand CALEA to require Internet service providers and other online services make their products amenable to Government surveillance and intercept. There have been recent published reports about draft legislative proposals circulating, although the administration has not sent anything up here.

Should I be expecting a specific legislative proposal from the FBI or the administration in the near future?

Mr. MUELLER. I believe you would, but I do believe that characterization is somewhat of a distortion of what our needs are. As was pointed out by Ranking Member Grassley, we will go to court, make the appropriate showing of probable cause that there is a need to capture communications of a particular individual, and a judge will issue an order.

What we are seeking is the ability to enforce that order and be able to obtain those communications, and what we are looking at is some form of legislation that will assure that when we get the appropriate court order, that those individuals, individual companies that are served with that order do have the capability and the capacity to respond to that order.

Chairman LEAHY. I think it would clear up a lot of confusion about what might be sought if we can actually see a proposal from the administration, and I would urge the administration to get that before us.

Senator GRASSLEY.

Senator GRASSLEY. I had a lead-in to my first question that I am going to skip, but it goes back to exactly the first question that the Chairman asked.

Do you know why the Justice Department did not notify defense counsel in each case of the task force's findings?

Mr. MUELLER. I am not certain that they did not—I am not certain exactly with specificity what the notification procedures were back in 2004. I would have to get back to you on that, who was notified and who was not notified and the circumstances under which a decision was made.

Senator GRASSLEY. Did the Justice Department share records with the FBI about what notifications went to the prosecutor?

Mr. MUELLER. I would have to check on that. I am not certain.

Senator GRASSLEY. Okay. Well, I hope if there is one area where we should all be able to agree, it would be on this one, that defense counsel ought to be notified or the person that is in jail ought to be notified if there is other information that might bear on the case. And, Chairman Leahy, I would like to work with you to bring some public accountability to this process, just as you and I worked together on the Army Crime Lab issue a while ago.

My next question deals with the airplane, but not your use of the airplane. It is a sensitive issue with you, so it is not about you.

Mr. MUELLER. Yes, sir.

Senator GRASSLEY. Last month, the Associated Press reported that Defense Secretary Panetta incurred \$870,000 in personal travel to California using a government plane. In accordance with OMB policy, Panetta reimbursed the Department for the flights, but at a significant discounted market rate. It is my understanding that the Attorney General utilizes FBI aircraft for official and personal travel. I also understand that the FBI is charged for these trips, along with other trips the Attorney General takes on non-FBI aircraft, such as DOD and FAA planes.

Does the Attorney General use FBI aircraft for both business and personal travel?

Mr. MUELLER. He is required to use FBI—not necessarily FBI, but he is required to use government aircraft so that he is in continuous contact, communications contact.

Senator GRASSLEY. Okay. Does the FBI charge the Attorney General's use of the FBI plane against its own budget or against the Attorney General's own travel budget?

Mr. MUELLER. I do think it goes against our budget, but I would have to check on that. The intricacies of the billing between the Department of Justice and ourselves for the security of the Attorney General I would have to get back to you on.

Senator GRASSLEY. Then the question comes: Why would the FBI be paying for this?

Mr. MUELLER. I would have to look at that. There is probably historical—or it may be we are responsible for his security wherever he is at whatever particular point in time, whatever transpor-

tation he uses. And how that is specifically billed I will have to go and check on.

Senator GRASSLEY. Okay. And it is my understanding, according to my friend on my left here, that this may have been a policy going back prior to this administration. If so, I still would like that information.

Then you will not be able to answer this, but I am interested in the cost, so include that in your answer to me.

[The information referred to appears under questions and answers.]

Senator GRASSLEY. And according to information provided me, the FBI may have had to lease a private plane because the FBI jet was reserved for senior Justice Department officials. Would that—

Mr. MUELLER. Both myself and the Attorney General, the Department of Justice and FBI, understand that these planes are first for investigative work. They are used for counterterrorism, criminal cases, and that any travel of the principals is secondary to the use of the plane for the investigative work of the FBI.

Senator GRASSLEY. I look forward to your responses to that. Thank you.

Now, on national security leaks, the FBI has reportedly opened an investigation into leaks about the recent underwear bomb operation. It is my understanding that the information that was leaked may have compromised the ability of the CIA and our partners to use the same sources and methods for similar operations in the future. I am particularly concerned if the operation tactics were leaked for political gain, as we have seen in the past, with the authorized leaks from the White House about the operation to kill Osama bin Laden.

Do you agree with me that this leak was damaging to our national security to fight terrorism?

Mr. MUELLER. Well, let me start by saying that we have initiated an investigation into this leak and also affirm, as I think you indicated before, that leaks such as this threaten ongoing operations, puts at risk the lives of sources, makes it much more difficult to recruit sources, and damages our relationships with our foreign partners. And, consequently, a leak like this is taken exceptionally seriously, and we will investigate thoroughly.

Senator GRASSLEY. Okay. I guess you have answered my question there, but the last point that you made was a point I wanted you to make, so I guess I would say, regardless of political consequences, I hope that you get to the bottom of it.

Our international partners have been wary of cooperating with us in the wake of WikiLeaks affair in which our ability to keep their confidence was severely damaged. What effect do you think the leaks in this case will have on our ability to work with allies in combating terrorism?

Mr. MUELLER. My hope is that it will have minimal impact, and I know that there are discussions that are going on with partners overseas to make certain that whatever impact there is is minimized and precautions put into place so that in the future does not happen again.

Senator GRASSLEY. Director Mueller, you have identified fighting terrorism as one of the main priorities, and in your written statement for this hearing, you identified FISA amendments as a crucial part. You have personally encouraged the reauthorization of the FAA, and your colleagues in the administration, DNI Clapper and Attorney General Holder, have sent letters and legislative proposals to accomplish that. I agree with you about the value of the FAA tools, and I support the clean authorization of FAA.

Could you please describe exactly why the FAA is so valuable? What authority does it provide that other statutes do not?

Mr. MUELLER. Well, at base, it provides the authority for intelligence agencies to gather or collect information on conversations overseas between persons overseas, non-U.S. citizens. And that intelligence is tremendously important to our ability to analyze and predict threats against United States citizens overseas, but also against the United States homeland itself. And absent that, we would be in the dark when it comes to identifying individuals and threats from numerous countries overseas that harbor, willingly or unwillingly, persons who want to do us harm.

One example I could give is the Najibullah Zazi case, which has been described by the Chairman as a recently—an aspect of it that was recently concluded in convictions in New York. That is a case that benefited dramatically from the benefits of the FAA.

Many of the other benefits would have to be discussed in a closed session.

Senator GRASSLEY. Could I have just one short follow-up?

A two-part follow-up: Is it critical that we reauthorize FAA this year? And is there sufficient oversight and checks and balances to ensure that the rights of U.S. citizens are protected?

Mr. MUELLER. Well, yes, it needs to be done this year so we are not in limbo as we have been in the past awaiting legislation, and hopefully not having it be carried for a month or so. But, absolutely, it is important that we get it and we get it quickly.

What was the second part of the question, sir?

Senator GRASSLEY. Is there sufficient oversight and checks—

Mr. MUELLER. Yes.

Senator GRASSLEY [continuing]. To ensure the rights of U.S. citizens being protected?

Mr. MUELLER. Yes, I do believe there is. I know the Inspector General's offices are very active in this, and also the Intelligence Committees as well as this Committee in terms of giving oversight to this particular program, and to assure, to the extent one can, that it is focused on those individuals who are communicating overseas and who are not U.S. citizens.

Senator GRASSLEY. Thank you very much.

Chairman LEAHY. Thank you.

Senator Kohl.

Senator KOHL. Thank you, Mr. Chairman.

Director Mueller, before I turn to my questions, I would like to thank you for your work to keep open the La Crosse, Wisconsin, FBI satellite office that, as you know, had been slated for closure. This decision will allow the FBI to do a better job at protecting western Wisconsin and continue the strong local and federal law

enforcement partnership there. I appreciate your willingness to be attentive to my interest in this issue.

Director Mueller, as we all know, this is National Police Week, and yesterday we honored officers who made the ultimately sacrifice. Included in the dozens of names to be added to the National Law Enforcement Officers Memorial this year is Officer Craig Birkholz of the Fond du Lac, Wisconsin, Police Department.

As we remember the sacrifices of these brave men and women, we need to ensure that law enforcement officers have the federal support and the resources they need to keep our communities safe.

Director Mueller, last week at a House hearing, you said that because of the FBI's realignment in priorities toward counterterrorism and limited resources, the FBI will have to "prioritize in other areas, and particularly in the criminal area they will suffer." Could you elaborate a bit on that comment?

Mr. MUELLER. Yes, I actually think that the question was directed on the impact of sequestration on the Bureau. I think the question was something along the lines of, what impact would sequestration have on the Bureau and how will you handle it? To which my response was that it will cut across all of our programs. It actually will—we will have to take a seven- to eight-percent cut across the boards, and when we do that, we have to prioritize. And the priorities we have are counterterrorism, counterintelligence, espionage is number two, and cyber are the three top national security, and you cannot, particularly in the cyber realm, cut there. So you have to look for cuts in the criminal programs.

Where we would end up doing it, I do not know, but one has to prioritize. We will lose something in the neighborhood of 1,500 personnel if sequestration goes there. That will be several hundreds of agents, almost 1,000 analysts, and almost 900 professional staff. It will be a very hard hit.

My answer was in response to a question about what would happen if sequestration follows.

Senator KOHL. How hard a hit will it be, in your judgment, with respect to your ability to do the job that the FBI is required to do?

Mr. MUELLER. Well, there will be gaps in what we are going to do. We will probably have to ratchet back in the white-collar criminal program. We have got thousands of agents now looking at health care fraud, mortgage fraud, securities fraud, and corporate fraud.

In terms of addressing gang violence around the country, we probably will have to cut back in terms of our task forces.

Our belief since September 11th has been we maximize our capabilities when we work in the context of task forces, so we have established hundreds of Safe Streets Task Forces where we will have one or two or three agents, but we will leverage our capabilities with State and local law enforcement. We will have to cut back in these areas, and that will have, I believe, an impact on those communities that do not have the capabilities of the Bureau leveraged with the State and local law enforcement to address violent crime on our streets.

Senator KOHL. Director Mueller, last month Al Qaeda in Yemen recruited a suicide bomber to blow up a U.S.-bound airplane with a sophisticated explosive device. Fortunately, the would-be bomber

was actually an informant working for Saudi Arabian intelligence and the CIA. This was a tremendous victory for the United States intelligence. We were able to unravel a major terrorist plot, recover a newly devised weapon, and obtain valuable intelligence.

But there appears to be a question as to whether this explosive device would have been detected by our current airport security screening. Even if our more sophisticated body scanners were able to detect it, not all domestic airports and only some international airports with U.S. inbound flights use them.

What are counterterrorism officials, including the FBI, doing to ensure that these types of devices do not make it onto airplanes?

Mr. MUELLER. Let me start by saying I have to—in this session, I cannot affirm the predicate for the question. I understand the question with regard to the device. What we are doing is working with TSA in particular to assure that any information we have which would bear on TSA and Department of Homeland Security's ability to pick up these devices is in their hands, so that we can make certain that we have the capability of alerting on these devices should another one appear.

Senator KOHL. Director Mueller, while counterterrorism remains, as you have said, your number one priority, the FBI also plays a central role in protecting American innovation and businesses from the serious threat of trade secret theft and economic espionage, which you referred to and which you estimated cost businesses billions of dollars every year. I am pleased that the FBI and relevant divisions within the Justice Department have increased the number of investigations by some 29 percent in the last year. This big jump in the number of investigations suggests that the problem may be even greater than we had previously thought.

Given the increase of investigations and the ever-growing threat to American businesses, jobs, and our economy, do you have the needed resources to continue to step up enforcement of economic espionage and trade secret theft? Can we expect to see an increase in these investigations and prosecutions?

Mr. MUELLER. An increase in investigations and prosecutions follows an increase in personnel. We have now over 50 individuals who are focused solely on these particular cases. We quite obviously have to prioritize the cases we tackle. One of the major ones we had over the last year was Megaupload, the takedown, as I think you are familiar with, of individuals in New Zealand. But we are utilizing those personnel to focus on the most egregious cases that we find and particularly those cases which could result in harm to persons if there are false or inadequately manufactured products that are being sold.

But going back to your point, this is a huge area. I cannot purport to say that we are making a huge impact on it. It would take additional resources. But we have to prioritize and lock people up as a deterrent to others engaging in this same activity.

Senator KOHL [presiding]. Thank you.

Senator Hatch.

Senator HATCH. Well, thank you, Mr. Chairman. Welcome, Mr. Director. I personally have appreciated your service over all these years. You were nominated by President Bush for a 10-year term. In 2001, you were subsequently and unanimously confirmed by the

Senate in September 2001. Your 10-year term was set to expire on September 4, 2011, but it was extended for an additional two years. I think that was a good thing to do.

Now, if I had my way, we would keep you right where you are. I understand——

Mr. MUELLER. My wife is not hearing this.

Senator HATCH. Since your term will expire next September, have you had any discussion with President Obama about potential successors?

Mr. MUELLER. I am sorry, sir?

Senator HATCH. Have you had any discussions with President Obama about potential successors?

Mr. MUELLER. I have in the past, but not very recently.

Senator HATCH. Do you have a transition plan in place for your successor?

Mr. MUELLER. Yes, we had put a plan in place so that we would be prepared for the new individual when that individual comes on board, and we are preparing for 2013 when we would expect a new individual to take the helm.

Senator HATCH. I figured you would.

Now, a great deal of attention has been paid to the case of Ali Musa Daqduq. He is a Lebanese national and Hezbollah field commander with ties to Iran. This terrorist orchestrated a brazen, botched kidnapping attempt in Karbala, Iraq, in 2007 which led to the death of five uniformed U.S. military personnel. Daqduq was in the custody of the United States military in Iraq from March 2007 until December 2011, when he was transferred to the custody of the Iraqi Government.

A *New York Times* report from May 7, 2012, indicates that an Iraqi court has ordered the release of Daqduq, citing insufficient evidence to prosecute him. The *New York Times* has also reported earlier this year that Daqduq has been charged with war crimes, including murder, terrorism, and espionage, before a U.S. military commission.

Is the FBI actively engaged with appropriate military officials on a plan to provide all necessary support and documents that would be needed for the prosecution of Daqduq before a military commission?

Mr. MUELLER. Well, yes, not only would we be willing and able to cooperate with a military commission if we obtain custody of Daqduq; in the meantime, however, we have cooperated with the Iraqi authorities in providing intelligence and information for their proceedings in Iraq with some of our agents testifying by civits in those proceedings. So we have tried to provide that information that we have to the Iraqi authorities in support of the Iraqi authorities' charges against Mr. Daqduq.

Senator HATCH. Okay. And you are going to follow up on that?

Mr. MUELLER. We will.

Senator HATCH. Okay. Your agency is conducting the investigation into the death of Border Patrol Agent Brian Terry on December 14, 2010. It has been a year and a half since this investigation began. In October 2011, Ranking Member Senator Grassley and House Oversight and Government Reform Committee Chairman Darryl Issa wrote to you inquiring about the status of that inves-

tigation, the number of weapons at the scene of the murder, and ballistic tests performed on the weapons recovered at the scene of the crime.

Now, your agency did not respond until May 4, 2012, and the FBI's response only indicated that press reports of a third weapon were inaccurate. There was no response to the other questions to include the status of the investigation. Can I ask you, what is the status of that investigation?

Mr. MUELLER. I can tell you it is an ongoing, very active investigation. Because of the seriousness of the offense and the loss of Agent Brian Terry, any personnel that are needed, it gets top priority. Because it is an ongoing investigation, I cannot get into the details. We have, when there has been a misperception out there of the facts of the case, tried to right them in the sense that there was a belief that there may have been a third weapon at the crime scene, and indeed there was not. There were two weapons recovered at the crime scene.

But going in at this point in time while the investigation is ongoing, it would be difficult to get into further details in this forum.

Senator HATCH. Would you be willing to tell us who at the Department of Justice is responsible for overseeing that particular situation?

Mr. MUELLER. Is the Department of Justice—in terms of prosecution, yes, it would be the Department of Justice that takes—

Senator HATCH. I am talking about who actually participated there in coming up with the idea and following through and giving these weapons to these—

Mr. MUELLER. Well, that would get into the details of the investigation, which I—

Senator HATCH. So you cannot get into that?

Mr. MUELLER. I cannot get into that here, sir.

Senator HATCH. Okay. You cannot tell us who at the Department of Justice was in charge of the—

Mr. MUELLER. I am not certain of the particular Assistant United States Attorney that is in charge. I am quite certain the Criminal Division would be in charge, but I know this investigation is a high priority for all levels of the Department of Justice and the FBI.

Senator HATCH. Okay. Well, the FBI has done great work in community outreach, particularly relating to fostering a relationship based on shared security goals. And given that the Federal Government has intruded into many aspects of our lives over the years, it is imperative that federal law enforcement carefully and continually articulate that the FBI is there to protect them, not police them for ordinary lawful conduct.

I want to bring to your attention a series of flyers from various FBI Joint Terrorism Task Forces. One of the flyers, which has received a great deal of attention, lists potential indicators of terrorist activities related to military surplus stores. Now, according to the flyer, customers who should be considered suspicious include those who demand identity private sector, insist on paying with cash, make bulk purchases of Meals Ready to Eat—MREs, in other words—and purchase weatherproof ammunition. Needless to say, there are many Americans who this could apply to who have noth-

ing whatsoever to do with terrorism, and they are rightfully concerned with this type of government decree.

Now, on the bottom of the flyer in the smallest print possible, the document reads: "Each indicator by itself is a lawful conduct and may constitute the exercise of rights guaranteed by the U.S. Constitution."

I think that disclaimer should have been very prominent and not hidden at the bottom of the page, and I think that this flyer and others like it needlessly send mixed messages and have raised alarm among citizens.

Can you confirm that the FBI is not looking at people who undertake such normal activities? And will you take an active role in the future by reviewing similar documents from FBI entities before they are released?

Mr. MUELLER. I will. We will. But I do want to put it in context. We do have what we call "tripwires" out there. For instance, at farm supply stores, ammonium nitrate, if somebody buys a substantial amount of ammonium nitrate far beyond what you would want for your garden or your fields, that is the type of thing we need to know about.

Senator HATCH. Right.

Mr. MUELLER. Other chemical, chemical companies, where persons are making purchases that are highly unusual. We had a circumstance where an individual down in Texas who was in the midst of constructing an IED purchased chemicals from a company that I believe was in Georgia or South Carolina. The company came to us and said this is highly unusual, and as a result of that tip, we were able to disrupt a substantial plot.

So we have a process out there. Clearly, having ammonium nitrate or camping gear in the lot in and of itself is not a crime. But I will—and I just came back to your question—go and review, have a panel review these to make certain that they are done appropriately.

Senator HATCH. Thanks, Mr. Director. I appreciate your service. You have given long and great service to this country. I appreciate it.

Mr. MUELLER. Thank you.

Chairman LEAHY [presiding]. Senator Feinstein.

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

Director Mueller, as Senator Hatch pointed out, you have served both a Republican and a Democratic administration. I have watched you carefully. You have never disappointed, and I think that is very impressive. I do not know whether this is going to be your last appearance before this Committee in the form of an oversight hearing or not, but I did want to say that to you directly.

Mr. MUELLER. Thank you.

Senator FEINSTEIN. You are welcome.

As you know, Title VII of FISA, the *Foreign Intelligence Surveillance Act*, expires December 31st of this year. This particular title allows for electronic surveillance of targets outside of the United States. The Senate Intelligence Committee, as well as this Committee, has done extensive oversight over the Government's use of these surveillance authorities, and we look forward to working with

you to reauthorize the FISA Amendments Act well before the end of this year.

I think we need to look no further than the recent AQAP bomb plot to know that the threat is still out there. As you said, it is very real, and there is no question that they will attack this country if they can.

For the benefit of Members and so that the American people can hear directly from you about this intelligence collection activity, can you please explain the need to reauthorize Title VII of the *Foreign Intelligence Surveillance Act*?

Mr. MUELLER. If we learned one thing on September 11th and one thing only, it was the need to share intelligence and gather intelligence to identify persons who would kill American citizens, whether it be here domestically or overseas. The shock of September 11th in part was attributable to the fact that these were individuals from outside the United States who were radicalized, who plotted, who then undertook the attack in the United States.

We cannot wait until the attackers are on the shores of the United States to preempt plots such as the plot that was preempted last week. We cannot wait until that person gets on the plane and is over U.S. territory in order to try to stop that plot. We have to know what is happening in Yemen; we have to know what is happening in the Fatah and Pakistan and Afghanistan; we have to know what is happening in Somalia; we have to know what is happening in Algeria and Morocco, because in each of these places there are pieces of Al Qaeda that are operating and are seeking to attack us domestically.

One of the key areas of insight into these activities is our ability to intercept conversations in a variety of media today and with the intercepted conversations, get a picture, an idea of what plotting is occurring overseas.

If you take that away from us, if you take that picture away from us, if you take away from us the ability to gather this kind of information, then we will be defenseless until a person crosses our borders, and we cannot allow that to happen.

Senator FEINSTEIN. Well, thank you very much. One of your legacies, of course, is going to be that you have put in place a very large intelligence component within the FBI. I gather it is above 10,000 people now working in intelligence. What is the actual number?

Mr. MUELLER. We have approximately 3,000 analysts, but all of our 14,000 agents now, in the intelligence community, you would call them "collectors." We call them "agents." But at the same time, they are collecting—whatever they do, they are collecting information. And whereas for the most part in the past we would focus on is it admissible in court, now it is information that is collected to fill gaps. What do we know about this particular threat to the United States? And what do we not know, and how do we fill those gaps?

And so, on the one hand, yes, we have 3,000 analysts. That has tripled since 2001. But also the organization as a whole understands that we address a threat. It is not just locking up people; it is not just putting people away; but it is understanding the threat and preempting the individuals who want to attack.

Senator FEINSTEIN. Do you know whether a crimes report has been filed with the Department of Justice pursuant to the AQAP bomb retrieval and the leak?

Mr. MUELLER. I am not certain—you describe a crimes report. There have been, I know, discussions between ourselves and other agencies as the necessity for and investigation on the leak. And as I have said, we have initiated an investigation.

In terms of reporting, we, as I think has been indicated, had the responsibility of exploiting the IED device, and whatever reporting has come out of that has gone to not only the Department of Justice but other agencies.

Senator FEINSTEIN. You have a counterterrorism special agent working out of Los Angeles that has been missing for five days now.

Mr. MUELLER. Yes.

Senator FEINSTEIN. What can you tell us about that?

Mr. MUELLER. We are still searching for that individual. His wife and the office sought yesterday to widely publicize the fact that he is missing. There have been searches made in those areas where this individual, this agent, would often run or hike. We are still searching.

Senator FEINSTEIN. Thank you.

On Sunday, Hank Crumpton, whom you probably know, the former head of the CIA's National Resources Division, was interviewed on "60 Minutes." When asked about counterintelligence—and I want to quote him—this is what he said: "If you look at the threat that is imposed on our Nation every day, some of the major nation states, China in particular, very sophisticated intelligence operations, very aggressive operations against the United States. I would hazard to guess that there are more foreign intelligence officers inside the U.S. working against U.S. interests now than even at the height of the Cold War."

Now, I know there is a limit to what you can say before this Committee, but how would you respond to that statement?

Mr. MUELLER. I think it is difficult to say, but I do believe the counterintelligence threat has evolved over a period of time. More generally, certain countries use far greater dispersal of individuals, and then as I mentioned in my opening remarks, the fact that so much of our data is kept in data bases on networks, and they may be vulnerable for attacks overseas, you do not have to be in the United States to undertake an attack and to secure secrets from our networks. And so the counterintelligence threat has evolved in ways that were not present back during the Cold War.

In terms of numbers of persons, I think that is less important than the ways that foreign countries are seeking to steal our secrets, not just within individuals, not just with "HUMINT," as one would call it in the intelligence community, but also with cyber attacks and cyber extractions of information.

Senator FEINSTEIN. One quick question. Sex trafficking of children.

Mr. MUELLER. Yes.

Senator FEINSTEIN. A big issue, large numbers, I think all of us one way or another have run into it in our States. What more can the FBI do to be helpful with this really terrible, terrible thing?

Mr. MUELLER. We have a program that we have had for a substantial period of time which we focus on this phenomenon throughout the United States, and we have, on a number of occasions, had substantial takedowns of individuals who are involved in it. Unfortunately, that does not end the problem. There are many more out there.

The gratifying aspect of it from persons who work there say it is that the victims we are able to save in terms of our activity. It is another area where we would love to be able to put more additional resources. We try to leverage what resources we have because every child saved is a child that we will remember for a good long time.

Senator FEINSTEIN. Thank you.

Chairman LEAHY. Thank you.

Senator KYL.

Senator KYL. Thank you, Mr. Chairman.

Just following up on that last point, you talked before about the need to prioritize in the event of sequestration. Every one of these responsibilities that the Federal Bureau of Investigation has are important to somebody, and in many cases, they are important to the entire citizenry.

When you said, "Our budget would take a big hit"—let me see if I can get the—"It would be a very hard hit" is what you just said. I recall when the Secretary of Defense was asked not just about the hit on the budget but the effect on the country on his ability to help defend the country. Could I ask you to respond to the question in that way about the FBI's ability to do the important work that it has? The Secretary of Defense called it "catastrophic." How would you characterize the effect of these sequestration across-the-board cuts if, in fact, they occur?

Mr. MUELLER. Let me go back and say I misspoke before, because I think I said it would be a seven- to eight-percent cut. I should have said we would lose 3,500 positions as opposed to 1,500. It is 3,500 positions: 1,500 special agents, 1,100 analysts, and 900 professional staff.

It is hard for me to categorize and use a word such as "catastrophic." I would say it would be, maybe as important a word, "devastating" for a variety of reasons.

Senator KYL. That is bad enough.

Mr. MUELLER. The individuals—and devastating from, as you point out, the impact it will have not just on the Bureau but on people that we serve. The programs that we have to save children, the programs we have to protect our networks from cyber attacks, the programs we have to put behind bars those persons who are responsible for white-collar crimes, securities fraud, corporate fraud, and mortgage fraud, health care fraud—all of which if you do not have the capacity to go and put the persons in jail, then there is no deterrence and it will grow. It will hamper that.

And more particularly, what people tend to forget is the long-term effects when you have a hiring freeze or you have a sequestration where the institution is impacted for years down the road. It may be rectified in 12 months or 18 months or two years. But that hiring freeze and the like translates into a gap in that agency for years down the road.

Where we are attempting to keep up with the technology when it comes to responding to cyber attacks, we will miss a generation of individuals who have those capabilities if we are required to cut back and lose 1,500 agents. So not only is the impact devastating at the outset, it is devastating down the road.

Senator KYL. Thank you for that, and I share my colleagues' concern that we must address this, and certainly before the end of the year.

Let me also refer to your testimony about investigating the source of the leaks of this most recent—I think you referred to it as an IED, but we can refer to it as another potential underwear bomber case. Would that be accurate?

Mr. MUELLER. Yes. Explosive device.

Senator KYL. Explosive device. And you do have an investigation ongoing, underway. Is that correct?

Mr. MUELLER. Yes.

Senator KYL. And let me just ask you about—how would you characterize how important it is to find the source of the leak?

Mr. MUELLER. As I indicated before, leaks such as this have a devastating—I do not want to overuse the word “devastating”—but have a huge impact on our ability to do our business, not just on a particular source and the threat to the particular source, but your ability to recruit sources is severely hampered. And in cases such as this, the relationship with your counterparts overseas is damaged, which means an inhibition in the willingness of others to share information with us where they do not think that information will remain secure.

So it also has some long-term effects, which is why it is so important to make certain that the persons who are responsible for the leak are brought to justice.

Senator KYL. Now, sometimes there is no other lead that leads you to the result except talking to the reporters involved. In the past, you and others in the law enforcement community have taken a very strong position indicating your concerns about legislation that would undermine your ability to protect intelligence sources and methods that could seriously impede national security investigations.

Is it still your view that it would not be a good policy for reporters to have a special privilege or a special right not to talk to FBI or other law enforcement officials if they may have the information that would lead you to the leaker?

Mr. MUELLER. That is somewhat general in terms of sort of framing legislation. I would have to leave the ultimate decision on the legislation to the Department of Justice. But I do believe that the protocols established within the Department of Justice to protect and assure the media are adequate to accomplish that task.

Senator KYL. I appreciate that, and the reason I ask the question generally is because I realize that policy is set by the Attorney General or the administration generally, which is why I asked you about as a general proposition whether it is helpful or harmful to your efforts. And you have said in the past that your FBI guidelines are sufficient. Others have agreed with that. I happen to agree with that and think that that is good policy.

Let me just conclude by reiterating the comments of both Senators Kohl and Feinstein about the importance of reauthorizing FISA before the end of the year. There is a lot of concern around here that we are going to kick all of the big, important decisions down the road to after the election, and even though this does not expire until the end of the year, I think my colleagues were saying it would be good to do this as soon as possible.

Just from the standpoint of knowing what you have to deal with in the future, the continuity of your training and law enforcement efforts and so on, is it your view that the sooner we could accomplish this reauthorization of Title VII of FISA, the better from your perspective?

Mr. MUELLER. Yes. Give us some certainty.

Senator KYL. Thank you very much, Mr. Director.

Senator FEINSTEIN. [Presiding.] Thank you very much, Senator Kyl.

Senator Durbin.

Senator DURBIN. Thank you, Senator Feinstein.

Director Mueller, good to see you.

Mr. MUELLER. Senator.

Senator DURBIN. And thank you for your service. You have done an extraordinary job in one of the most challenging times in our Nation's history. I thank you personally for taking some time to focus attention on my home town of East St. Louis, Illinois, which, sadly, has one of the highest rates of violent crime per capita in the Nation. There is a WAVE Task Force, a multi-unit task force, including FBI agents, which is doing its level best to change that, and I thank you for your willingness, even with limited resources, to participate.

We have exchanged conversations and correspondence on the issue of training manuals, and I would like to make the record clear today about the current situation. I am asking to enter into the record letters which you and I exchanged in March and April of this year when it was disclosed, when some parts of the training manuals became public, that some things had been stated in the training of FBI agents which had been, I would just say, characterized as inappropriate and unfair to Arabs and Muslims. And we have spoken about this personally. I have spoken to Attorney General Holder. Could you tell me at moment in time what is the current status of training manuals in the FBI as it relates to these two groups and what you have done to make certain we do not have the kinds of things that have troubled us in the past?

Mr. MUELLER. Yes, Senator, as I have indicated in the letter, when this came to our attention last summer, we took it exceptionally seriously, and we convened a group of five individuals, we believe, all of whom have advanced degrees, two of whom were in the Bureau, three were outside the Bureau, to make a preliminary review of the materials and determine what then should be done to make certain that the training we give our agents is appropriate.

With a touchstone document—and I have to apologize because I believe in a conversation with you I indicated that it was a curriculum. It was not. It was a touchstone document that these persons put together as a guidance as to how to go through and treat the records we were going through.

We then had up to 30 individuals—agents, analysts, and others—go through over 160,000 documents, training documents—not necessarily a manual but training documents that had been used over the preceding 10 years since September 11th, along with more than 1,000 slides and the like. We had them go through and pull out those particular documents that were inappropriate for whatever reason. They could have been wrong; they could have raised the specter of an individual being pointed out that should not be pointed out. For whatever reason, those particular documents needed to come out of our training. We identified 876 of those documents that needed to be pulled out. We found the other approximately 160,000 documents appropriate.

Then, with those documents, we went out to the field and explained why these particular documents, with examples, were inappropriate. We interviewed the individuals who were responsible for those documents. We did more than 100 interviews of such individuals. And we also are in the process now of going out and making certain that the materials that we are using are in accordance with our—are appropriate.

One of the things it did teach us and one of the things that comes out is that we did not have a mandatory review for training documents such as this, and so we have put into place, apart from this, a review of training so that anybody who is giving a training cannot just go up and put together their training materials. It has to go through a screening process.

We have taken it exceptionally seriously, as I think perhaps you can understand given the personnel we put on it. But I think we have gone a long way to resolving the issue.

Senator DURBIN. Critics have said this is all about congressional meddling and political correctness, and I would like to have your characterization, because you stated to us earlier that one of the key elements in fighting terrorism is connections, cooperation, and you have said, Attorney General Holder has said that Muslim Americans and Arab Americans have been a vital part of our effort to keep our Nation safe. I would like to have your characterization as to whether this is just an exercise of political correctness.

Mr. MUELLER. Well, for us and for me personally, it is not an exercise of political correctness. It is an exercise of doing what is right given what we had seen. I believe that the five individuals that we selected have the professional capabilities to guide us in this way, and it is absolutely essential that our agents are instructed giving the best possible materials and those materials that are in accordance with our core values. So I reject any assertion that this is as a result of political correctness or any such other characterization. It is what needed to be done. And I will follow up, as I have before, and said that many of the cases that we have done are a result of the Muslim community bringing to our attention individuals who needed further investigation, and we would not be as safe as we are today without the support of the Muslim American, Arab American, and Sikh American communities in the United States.

Senator DURBIN. Thank you. I only have a brief time left here, and I am sorry because we went through this exercise—and it was unusual—where all Members of the Senate, Democrats and Repub-

licans, were invited to a classified hearing—the FBI was represented, the Department of Defense, so many other agencies—on cybersecurity, which you mentioned. There is a bill pending to try to make our Nation safer from the cybersecurity threat. I am trying to look at this through the prism of our individual rights of privacy as individuals and the basic liberties and values that we share.

Can you tell me, in the brief time remaining here, do you feel that the cybersecurity legislation proposed by the administration compromises any of the rights of privacy that individuals have customarily enjoyed in this country under wiretap statutes and other—I could go through the specifics here—other legislation? Are we changing the standard when it comes to cybersecurity in terms of the disclosures of any individuals' emails or texts in the name of security?

Mr. MUELLER. It does not change the standards by which the government can obtain information relating to an investigation. Let me just put it that way. And while I am somewhat familiar with the administration's proposal, I am not thoroughly familiar, so I do not think from what little I know that it changes that dynamic at all.

I will say, though, the only way to prevent a cyber attack, a substantial cyber attack, is to exchange information. In the same way, to prevent terrorist attacks you need to exchange information. And the success, any successes after September 11th are due to the fact that we are working closely with State and local law enforcement, working with the intelligence community. We understand that the borders no longer protect us, and we have to share information. To protect against cyber attacks, we are going to have to do the same thing, but it is going to have to incorporate the private sector in ways that you did not have to incorporate the private sector when we were facing the counterterrorism threat.

But the cyber threat will be no less than the counterterrorism threat. There will have to be the exchange of information, and it needs to have an exchange not just between the intelligence community and the law enforcement community, but between the intelligence community, the law enforcement community, DHS, and the private sector.

Senator DURBIN. There will be many more questions. I thank you.

Chairman LEAHY. Thank you.

Senator Lee.

Senator LEE. Thank you, Mr. Chairman.

Thanks for joining us today, Director Mueller, and I want to thank you not only for being here but also for serving our country. Yours is not an easy job.

Last year, you expressed some concerns about the National Defense Authorization Act for 2012. Specifically, in a letter that you wrote to Senator Levin in November of last year, you expressed some concerns with what became Section 1022 of that legislation, saying that you were worried about that provision introducing a degree of uncertainty and potentially inhibiting the FBI's capacity to convince covered arrestees to cooperate immediately and to provide important intelligence.

My concerns with the NDAA focused much more with what became Section 1021. To some extent, I think the President indicated that he shared some of those concerns. He indicated in his signing statement on December 31, 2011, as follows. He said, "I want to clarify that my administration will not authorize the indefinite military detention without trial of American citizens. Indeed, I believe that doing so would break with our most important traditions and values as a Nation. My administration will interpret Section 1021 in a manner that ensures that any detention it authorizes complies with the constitutional laws of war and other applicable law."

In light of that statement—you know, I was encouraged by that statement. I think it is good. I still had some concerns that future administrations might not hold that view or that this administration might change its position at some point. In light of that concern, I joined with Senator Feinstein in introducing S. 2003, the *Due Process Guarantee Act*, to ensure that U.S. citizens apprehended on American soil are not detained indefinitely without charge or without trial.

So I guess my first question is: Do you share the President's commitment, as I assume you would, as to the fact that U.S. citizens should not be detained indefinitely without trial under 1021?

Mr. MUELLER. Well, yes, in the sense that—yes. Yes. But let me just say there is no change to our activities; in other words, our authorities remain the same. How we handle things is not changed by the President's declaration. But, yes, I would assume that that would happen, that would be the case.

Senator LEE. Some people have suggested that military detention may be necessary in some of these circumstances because FBI and other civilian authorities lack the resources or the capabilities to deal with the unique circumstances associated with the apprehension and detention of terrorism suspects. And so my question for you on that point is: What are the FBI's abilities in this regard? Do you feel the FBI would lack the capacity to handle these circumstances to deal with the apprehension and detention of terrorism suspects?

Mr. MUELLER. No. The answer at the outset is no, but we may be talking about a different class of—if you are talking about covered 1022 persons, we are talking about individuals who are non-U.S. citizens, individuals who are participating in a plot with Al Qaeda and the like, where 1022 kicks in.

Going back to your initial question, I had some concerns about clarity as to what would happen at the time of arrest. Those concerns have been put to rest by the protocol that was established by the President.

Regardless of whether a person is detained in the United States by the FBI or ultimately it could be by the military, if it happens on a base, for instance, I have no question but that ourselves and the military would be capable of handling the consequent investigation and search for intelligence.

Senator LEE. Okay. So given this protocol that was developed in light of the President's signing statement on December 31st, given what you just added to that, would it be fair for me to assume that the administration would not object to legislation that would put

this rule in place by statutes, in other words, to say that we would not use Section 1021 to indefinitely detain U.S. citizens?

Mr. MUELLER. That would have to go to the Department of Justice. That is a step too far for me.

Senator LEE. Understood. Understood.

In your testimony, in your written testimony, you stated that you support the reauthorization of the FISA Amendments Act. Among other things, those amendments authorize the government to surveil various categories of non-U.S. persons abroad, outside the United States, without the need for a court order for each individual target.

Although these amendments do not appear to allow the government intentionally to target a U.S. person or intentionally to target any person on U.S. soil, it does seem that the amendments have the potential to result in warrantless surveillance of communications that involve U.S. citizens.

Can you explain, in light of this potential, what steps can be taken, what steps might be taken in order to protect U.S. citizens?

Mr. MUELLER. Let me just say we are concerned about both the thrust of the statute as well as the provisions of the statute that minimize the possibility of this happening. But beyond that, I would have to do it in closed session.

Senator LEE. Okay. But you do share the concern that there is that potential and you share a commitment to taking steps to protect U.S. citizens?

Mr. MUELLER. Yes, and my understanding is as the statute was winding its way through Congress, those concerns were raised and addressed in the statute. And, yes, we fully comply and understand the thrust as well as the letter of the statute.

Senator LEE. Okay. I see my time has expired. Thank you, Mr. Chairman. Thank you, Director.

Mr. MUELLER. Thank you.

Chairman LEAHY. Thank you, Senator Lee.

Senator Blumenthal.

Senator BLUMENTHAL. Good morning, and I want to join other Members of the Committee in thanking you for your extraordinary service over many years, many challenging and difficult years, on many challenges and difficult topics. Obviously, particularly in the area of terrorism, the FBI has taken an increasingly important role not just in terms of apprehending and prosecuting terrorism here in this country, but also abroad. And in the area of white-collar crime, you have continued to be an extraordinarily important presence.

I would like to ask first about the JPMorgan Chase investigation. Can you tell us what potential crimes could be under investigation without asking you to conclude anything or talk about the evidence? Would it be false statements to the Federal Government or what area of criminal activity?

Mr. MUELLER. I am hesitant to say anything other than what is available under Title 18 or available to the SEC would be the focus of any ongoing investigation.

Senator BLUMENTHAL. And can you talk at all about the timing of that investigation?

Mr. MUELLER. All I can say is we have opened a preliminary investigation, and as you would well know, having been in this business for a long time, it depends on a number of factors.

Senator BLUMENTHAL. And I am not going to press you further, but I would just encourage you, without your needing any encouragement, I am sure, to press forward as promptly and expeditiously and aggressively as possible, because I think that the American public really has lost faith in many other enforcement agencies, partly because of the delay and lack of results, and I think that the FBI's involvement is a very constructive and important presence in this area.

Mr. MUELLER. Thank you.

Senator BLUMENTHAL. Turning to the *Violence Against Women Act*, where, again, the FBI has really been a leading role in stopping assaults and intimidation and harassment of women. As you know, the Senate has reauthorized VAWA—it is now under consideration in the House—with provisions on cyber stalking that seem less forceful and robust than the ones that we adopted and I have urged and drafted to adopt in this body.

I wonder if you could talk to us about how important cyber is in the area of domestic violence and violence against women generally.

Mr. MUELLER. Well, I must say I am not familiar with the differences between the two proposed statutes. I will say, on the other hand, that cyber stalking is—it can be difficult to define, but once defined, the impact is substantial on the individuals, and it is a growing phenomenon that does need to be addressed.

Senator BLUMENTHAL. And would you say that crimes resulting in domestic violence or violence against women do often involve the Internet and the use of impersonation and similar kinds of tactics?

Mr. MUELLER. Increasingly, and increasingly, once you have one individual who is prosecuted for this and it becomes public, you find a number of others that would undertake the same activity, unfortunately.

Senator BLUMENTHAL. Thank you.

Turning to another subject, drug shortages. I do not know whether you are familiar with some of the gray market activities, some of the potential price gouging that goes on with respect to pharmaceutical drugs that are in shortages—cancer treatment, anesthesiology drugs. The FDA was ordered by the President to refer to the Department of Justice any evidence of drug shortages that could involve either civil or criminal violations of law. I wonder if you are familiar with any cases that have been referred.

Mr. MUELLER. I am not, but we may well have cases that I am not familiar with or aware of relating to this particular area.

Senator BLUMENTHAL. If you could get back to me on that subject and if you feel you are at liberty to do so, that would be helpful.

Mr. MUELLER. I am happy to do that.

Senator BLUMENTHAL. On the ongoing investigation—I take it it is ongoing—with respect to East Haven in the State of Connecticut, is there any update that you can provide? And I just want to say before you answer that both the FBI and the United States Attorney's Office and, in particular, the United States Attorney in Connecticut overall, as well as on this case, are doing extraordinarily

excellent work, and I am very proud of the great job that they are doing there, and I say that as one who would be critical—having been a United States Attorney, I am not one who would be less than demanding of that office, but they are doing—both the FBI and the U.S. Attorney there are doing great work.

Mr. MUELLER. I am familiar with the investigation but cannot in open session discuss it.

Senator BLUMENTHAL. On gasoline prices, do you know of any uptick in criminal activity there with respect to price gouging or—

Mr. MUELLER. Have not. Again, that is something we will have to get back to you on. We may have seen something. I would have to go back and find out where we are on that.

Senator BLUMENTHAL. Thank you. Again, thank you for your great work. My time has expired, and I appreciate your being here.

Mr. MUELLER. Thank you.

Chairman LEAHY. Thank you very much.

I yield now to Senator Graham, and I was going to ask Senator Blumenthal if he is willing to take the Chair, as I will not be coming back. I am going on to something else. Again, as I told you earlier, both publicly and privately, Director Mueller, I appreciate your cooperation. And some of the things, as you have said, will have to be in closed session. We can follow up with you privately.

Mr. MUELLER. Thank you.

Chairman LEAHY. Thank you. Senator Graham.

Senator GRAHAM. Thank you, Mr. Chairman.

Thank you again for your service, Director. I am going to send you a series of questions to kind of explore further what Senator Lee was talking about so we will not have to use the whole seven minutes here talking about the details of Miranda and what an enemy combatant is or is not. But we are going to talk about big themes.

On cybersecurity, do you have all the resources you need right now to defend the Nation against a cyber attack within reason?

Mr. MUELLER. We need additional resources. We are reprioritizing. We are reorganizing to address cyber. We have a—

Senator GRAHAM. What is the risk to the Nation of a cyber attack in the next decade?

Mr. MUELLER. Substantial.

Senator GRAHAM. So would you do me a favor and just quietly and appropriately write down that list of needs and get them to me, and I will spread them to my colleagues.

Mr. MUELLER. Have done it. Will do it.

Senator GRAHAM. And I just really appreciate the FBI in many ways.

Senator GRAHAM. Okay. Do you believe that we are in a war against terrorism? Is the war on terror an appropriate name to define the time in which we live?

Mr. MUELLER. Yes.

Senator GRAHAM. Okay. I do, too. It is not the crime on terror. It is the war on terror.

I believe that Article III courts have a place in prosecuting terrorists. Do you agree with that?

Mr. MUELLER. Yes.

Senator GRAHAM. Do you believe that military commissions could also have a place in prosecuting terrorists?

Mr. MUELLER. Yes.

Senator GRAHAM. U.S. citizens are not eligible for military commission. Do you agree with that?

Mr. MUELLER. Yes.

Senator GRAHAM. Just say yes because—okay.

[Laughter.]

Senator GRAHAM. I am not trying to trick you.

Mr. MUELLER. I am waiting.

Senator GRAHAM. I know, I know.

Is the homegrown terrorist threat growing or lessening?

Mr. MUELLER. Growing.

Senator GRAHAM. Do you consider America part of the terrorist battlefield, the country itself? Isn't that sort of what they want to do, is hit us here as much as anywhere else?

Mr. MUELLER. You know, one could get into parsing the terms of the description. I would say that we have a terrorist threat domestically, and we have terrorist threat internationally.

Senator GRAHAM. Right. Well, let us talk about the fact that I think they want to kill us everywhere, but particularly here, and I do not think it was an accident that they brought down the Twin Tower, attacked the Pentagon, and tried to attack the Capitol. They are coming after us. Do you agree with that?

Mr. MUELLER. Yes.

Senator GRAHAM. All over the world.

Mr. MUELLER. Yes.

Senator GRAHAM. And we have a right to defend ourselves.

Mr. MUELLER. Yes.

Senator GRAHAM. Within our values. You do not support waterboarding, right?

Mr. MUELLER. No.

Senator GRAHAM. Nor do I.

Mr. MUELLER. It does not comport with our guidelines.

Senator GRAHAM. I agree, and I appreciate you at a time when it was not popular saying so, quite frankly.

Do you believe Khalid Sheikh Mohammed is an enemy combatant?

Mr. MUELLER. I am not going to—I will go down the road just so far, but in terms of the designation, I think there are a number of factors that go into that, so I am not going to say a yea or a nay.

Senator GRAHAM. Well, do you believe that Al Qaeda members can be classified as enemy combatants since we have about 200 and some at Guantanamo Bay?

Mr. MUELLER. I believe so, but, again, this is dependent—

Senator GRAHAM. We are not holding people illegally there, are we?

Mr. MUELLER. No.

Senator GRAHAM. Okay. Now, if you caught Osama bin Laden or KSM or somebody like that tomorrow in the United States, would you suggest that the country take off the table military commission trials simply because the foreign terrorist was captured in the United States?

Mr. MUELLER. I would stay away from suggesting—that would be a decision for the President. My responsibility, our responsibility, would be to gather whatever facts, intelligence, and/or—

Senator GRAHAM. Right. Well, I am glad to hear you say that, because I do not believe it is the policy of Obama administration that foreign terrorists captured in the United States cannot be tried by military commissions and cannot be held as enemy combatants. And to Senator Lee's line of inquiry, I do not believe we want to send a signal to the world that if you make it to America, all of a sudden you get a better deal than if we catch you in Pakistan.

But let us talk about your job. When we capture someone that we believe to be affiliated with Al Qaeda in the United States, is it the Obama administration's position, the FBI's position, that those individuals captured collaborating with Al Qaeda in the United States must be Mirandized?

Mr. MUELLER. There is no blanket rule on Mirandizing individuals of Al Qaeda in the United States.

Senator GRAHAM. Well, okay. This is a very important. I think that is a good answer. Sometimes maybe it is the best thing to do; sometimes maybe it is not.

Mr. MUELLER. Well, I think the policy that has been laid out is that intelligence comes first.

Senator GRAHAM. Okay.

Mr. MUELLER. And the *Quarles* exception to the Miranda rule, we have leeway to undertake—

Senator GRAHAM. Okay. Right. How long under *Quarles*—which had to do with a domestic crime, not a terrorism case. How long can you hold someone under the *Quarles* case before you have to read them their Miranda rights?

Mr. MUELLER. I think that is still an open question.

Senator GRAHAM. Is it two days? Is it two weeks?

Mr. MUELLER. It is an open question depending on the circumstances.

Senator GRAHAM. Well, I would suggest that the people we have held at Guantanamo Bay for years as enemy combatants could only be held that long because we have designated them as enemy combatants. I do not want to bastardize the criminal justice system. Once we use it, I want it to work the way it should. And I believe that if you capture someone in the United States and you are going to charge them with a crime in an Article III court and that is your intent, your ability to hold them without Mirandizing them under *Quarles* is limited. But how long can you hold someone that you want to put in the criminal justice system without presenting them to a federal court under the presentment requirements?

Mr. MUELLER. You are required to present them generally within the next 24 or 48 hours.

Senator GRAHAM. Okay. So you have got to present them to court—

Mr. MUELLER. I presume you are talking about non-U.S. citizens.

Senator GRAHAM. Yes.

Mr. MUELLER. Okay.

Senator GRAHAM. So as I understand, then they get a lawyer at presentment, don't they? They have to have somebody helping them—

Mr. MUELLER. It depends on the circumstance. Some have, some have not.

Senator GRAHAM. Okay. But my point is that you are taking a suspect who we believe is involved in terrorism, when you put them in the criminal justice system, you have Miranda issues and presentment issues. If you keep them in the law of war system, holding them as an enemy combatant for intelligence-gathering purposes, you do not have these problems. Is that correct?

Mr. MUELLER. I am not certain to what extent you can make that blanket statement.

Senator GRAHAM. Okay.

Mr. MUELLER. And, also, I think there are downsides from doing it that are often overlooked.

Senator GRAHAM. Do you know any requirement in the law of war to read an enemy prisoner their Miranda rights or provide them a lawyer when they are held in military custody?

Mr. MUELLER. I am not familiar—I am not as familiar with the military code as you are.

Senator GRAHAM. Well, I would just suggest—and I do not want to belabor this, but we have never in a war captured an enemy prisoner and said, “Hey, you got a right to a lawyer, here is your lawyer. We hold you to gather intelligence because we are trying to prevent the next attack, not prosecute you.”

So I am going to send you a series of questions, and I want us to understand as a Nation that we are at war. I want to treat people fairly. I believe in all of the above. But I am not going to sit on the sidelines and go back to a pre-9/11 model of where the criminal justice system is the only tool available to fight this war.

So, Mr. Director, you have got really dedicated agents who are putting themselves at risk, and when we capture one of these people who we believe is involved with Al Qaeda in a way to hurt us all, I think we should have as many options as possible within our values and within the law of war and the criminal justice system to defend ourselves. So I am going to send you some questions, and I am glad to hear that there is no blanket requirement by the FBI to Mirandize a terrorist suspect upon capture in the United States. So that is good to know.

[The questions of Senator Graham appear under questions and answers.]

Senator GRAHAM. Thank you.

Senator BLUMENTHAL [presiding]. Senator Schumer.

Senator SCHUMER. Thank you, and thank you, Director, for the outstanding job you and the men and women who work for you do. I admire it every day.

Now, I would like to talk a little bit about relations between the FBI and the NYPD. Overall, it has been a great relationship; it has been a smooth relationship. It has been, I think, pointed to as an outstanding example, the Joint Terrorism Task Force, of cooperation between the Federal Government and State government and local government. But over the last few months, there have been a number of things that create a growing concern that that relationship may be fraying a little bit, particularly in regard to information sharing, which I know, obviously, you have got to be very

careful with, but these are two law enforcement agencies involved together in fighting terrorism.

There have been cases where the NYPD believes it has not been briefed on the specifics of terrorist plots, which is the type of information they need because of New York City being a top terror target. The Joint Terrorism Task Force should know information regarding terror plots related to New York City at the same time the FBI knows of this information or to give our forces the best chance to combat terrorism. And if it cannot be known immediately, it should be shortly thereafter.

We have some examples where for four or five days after it was even made public, they did not get the kind of detailed information that they wanted.

So my question is: Do you believe there is currently a problem hindering communication within members of the Joint Terrorism Task Force? If there is a problem, what can be done about it to better facilitate communication between the two? I have great respect for both and have been proud of the cooperation. If there is no problem, will you commit today to keeping NYPD abreast of any and all future developments related to terrorist plots? And will you work with the NYPD to address the cooperation and information-sharing issues so that everybody is on the same page and can work together as well as they have in the past?

Mr. MUELLER. Well, let me just start by saying that I think we have a very good relationship with the New York Police Department, particularly on the Joint Terrorism Task Force. We have tens of NYPD officers who have served on it. Many of them served for any number of years.

To the extent that the New York field office gets terrorism information, it goes to the Joint Terrorism Task Force.

Senator SCHUMER. Right.

Mr. MUELLER. It is there. The officers from the NYPD get the information at the same time as the agents on the task force get the information.

There are occasions where there is something very tightly and closely held in agencies, and it may be in Washington, that it takes some time before there is further dissemination, which makes sense. There are always bumps in the road. The——

Senator SCHUMER. Have they increased over the last months?

Mr. MUELLER. No, I would say——

Senator SCHUMER. It seems to me they have.

Mr. MUELLER. No, no. There are always bumps in the road, and every six months or so, Ray Kelly and I get together and discuss those bumps in the road and move on. So I think the relationship is very good and, let me just say, tremendously effective. I think the Joint Terrorism Task Force is effective. I think NYPD is effective at preventing attacks. And whenever you have strong-willed agencies and parts of agencies, you are going to have, as I say, the bumps in the road. I do not think there is any extraordinary action that needs to be taken by myself or Ray Kelly or others to address a current issue.

Senator SCHUMER. Okay. And that would apply in reference to—I understand the difficulties, as I read in the newspaper. I did not know anything else. The information about the recent airplane

bomber leaked out prematurely. You do not have to comment on that, but are there any problems with communication on that issue now between the——

Mr. MUELLER. There should not be.

Senator SCHUMER. There should not be, okay, because there was some talk that there was.

Mr. MUELLER. I heard that talk.

Senator SCHUMER. Okay. And have you talked directly to Commissioner Kelly about this?

Mr. MUELLER. I have not on this issue. I met with him about a month ago.

Senator SCHUMER. Would you be willing to?

Mr. MUELLER. Sure.

Senator SCHUMER. Great. Just a suggestion for the continued co-operation, give him a call on this, okay? He did not ask me to ask you to do that. I am. Okay?

Mr. MUELLER. Yes.

Senator SCHUMER. Thanks. And then one——

Mr. MUELLER. As I told Ray, he is always, you know——

Senator SCHUMER. I know. Let us not get into who calls whom. I am asking you to call him.

Mr. MUELLER. I am happy to do it.

Senator SCHUMER. Thanks. Appreciate it very much.

There was one other instance. This was not related to the Joint Terrorism Task Force, but you and I talked a little about this, and I did not follow up. When the FBI Bureau Chief in Newark publicly criticized the NYPD for conducting operations that he said made it more difficult to protect the public in New Jersey—again, I do not have a problem if the FBI thinks the NYPD is doing something that interferes with this operation in New Jersey. I was sort of surprised that he made it public. Now, what was that all about? That does not help.

Mr. MUELLER. I understand, and I have addressed the issue.

Senator SCHUMER. You have addressed the issue?

Mr. MUELLER. I have addressed the issue.

Senator SCHUMER. Okay. And everyone is happy now?

Mr. MUELLER. Not everyone.

[Laughter.]

Senator SCHUMER. Should I ask——

Mr. MUELLER. I have addressed the issue.

Senator SCHUMER. Okay. I hear you. Let us go on to another subject. Thank you. I am glad you have addressed it, and I hope that does not create any future problems, because it did create bad blood for a period of time.

Mr. MUELLER. I understand.

Senator SCHUMER. Okay. Stand your ground laws, there has been a lot of news this week about the FBI investigating hate crime charges in the Trayvon Martin case. I do not want you to comment on the investigation, but I just want to get your opinion about the stand your ground laws. Are they creating more violence than they are preventing?

Mr. MUELLER. I really cannot—there is that one incident we have. There may be others around the country. I cannot give you an opinion on that.

Senator SCHUMER. Okay. How about your general opinion on these stand your ground laws?

Mr. MUELLER. I do not know enough about them to render an opinion.

Senator SCHUMER. Okay. I would ask you, if you—again, I do not want to put you in any jeopardy in terms of this investigation, but if you wanted to think about it and had something in writing you wanted to send within the timeframe that the Chair has laid out, I would appreciate it.

Mr. MUELLER. Yes, sir.

Senator SCHUMER. I tend to think these are counterproductive and hurt law enforcement.

Okay. I have only 33 seconds left, so I will just submit my final question in writing.

Mr. MUELLER. Thank you.

[The question of Senator Schumer appears under questions and answers.]

Senator BLUMENTHAL. Thank you, Senator Schumer.

Senator Whitehouse, I—

Senator WHITEHOUSE. Let Senator Klobuchar—

Senator BLUMENTHAL. I am sorry. Senator Klobuchar is next. I am going to yield the gavel to Senator Whitehouse.

Senator WHITEHOUSE. I will be right back.

Senator BLUMENTHAL. As soon as he returns, and now Senator Klobuchar.

Senator KLOBUCHAR. [Presiding.] Thank you very much. I am the one standing with the gavel, I guess.

Senator BLUMENTHAL. You now have the gavel.

Senator KLOBUCHAR. Thank you, Director, for being here. I appreciate how often you come and how we are really kept abreast of everything that you are doing. Many of my colleagues have asked about officer safety issues with the national memorial services this week. I was just with the families and police officers over the last two days, two officers that died in the line of duty in Minnesota; one, in fact, reported to a scene of a domestic violence case, a 17-year-old victim, he basically sacrificed his life for hers, and he leaves three young children.

One of the things that came up at a previous hearing we had here on the bulletproof vest, which is incredibly important, is that 72 of our Nation's law enforcement officers were killed in the line of duty during 2011, and that is the highest number since 2007. It is up 20 percent from 2010. By region, 29 were killed in the South, 21 in the Midwest, 10 in the West, 10 in the Northeast, and two in Puerto Rico.

Are you aware of any factors that would explain this increase? Or do you think it is just random tragic statistics? Or do you know how this has happened?

Mr. MUELLER. No, I do not think anybody has a clear answer, although we tried to dissect those figures. I will tell you, as I indicated before, there are two things we are doing trying to reduce it.

The first is we have changed our pistol qualifications, understanding based on our data that many of the encounters that police have with persons with weapons are at a very short distance, not at a longer distance. And, consequently, we have to increase our ca-

pability of responding in shorter distances. And often when we change our protocols, State and local will follow as well.

Then, second, when an individual is stopped, and they go into NCIC to find out the record, we will put a warning in the record if the person has—a warning with a response if the person has a violent criminal history, to alert that officer to beware.

Senator KLOBUCHAR. Very good. Thank you. And I know we have discussed the bulletproof vest issue, how important that is, and I had not known until we had a hearing with some of our police leaders about the issue with women with bulletproof vests and how they need different bulletproof vests, which makes sense, and how sometimes they do not have those, as we are seeing more and more women police officers. But I wanted to note that to you.

Mr. MUELLER. Yes.

Senator KLOBUCHAR. It is something that we need to address.

I also know the FBI works closely with State and local authorities to keep our children safe through programs like the Child Abduction Rapid Deployment Teams and the Innocence Lost National Initiative. And next week, I am chairing a hearing on the issue of training child protection professionals. We have a good center in Minnesota, the National Child Protection Training Center in Winona, and one of the critical areas of training is forensic interviewing because many times a child victim may also be the only witness in these crimes. And according to one FBI child interviewers, methods used in adult cases may actually be counter-productive with child victims.

I know the FBI has been doing some good work in this area, and as a result, the FBI child forensic interviewers' expertise is in demand across the country. Could you tell me how the training is available to FBI agents? And what else can we do to help the FBI make progress on the problems of child abduction and abuse?

Mr. MUELLER. We have four child forensic interviewers who are very qualified and do great work. They get too much of that work, unfortunately, and build up that expertise. We provide training to agents and task force officers around the country. Generally, the training lasts from three to four days, and the statistics for 2011 are that we trained 650 agents and task force officers in 2011 alone, and we will continue that.

To the extent that there are law enforcement agencies that would benefit from that training, I am sure the special agents in charge in those particular divisions would try to accommodate.

Senator KLOBUCHAR. Well, thank you very much. I was just thinking back when I did a case as a prosecutor and it was a non-violent minor case, and there was a five-year-old witness. And without having any of your investigative skills, I put her on the stand and asked her what had happened, and I said, "Now, do you know what the truth is?" She said, "Yes, I do." And she said, "But when I was four, I always told lies" She was five years old, so I probably could have had an investigator, and needless to say, the case did not go very far.

Metal theft, this is something that I have been frustrated with. We have been trying to get a bill done. We introduced one last year, Senator Hatch and I did, on trying to look at some of the criminal penalties and trying to get some requirements in place

when scrap metal dealers get copper and other things, which we know sometimes can be stolen and sometimes now, with requirements for IDs and other things in place. And I just wondered if you are aware of that problem around the country with buildings blowing up and other things because of stolen copper.

Mr. MUELLER. Yes, and it is a problem. I will not mention the cities, but I know it is a problem in certain cities, and such a problem that emergency services can be adversely impacted by such thefts. And generally what we do is if there is a discrete group or entity that is involved in them, then we work with the State and locals to put together a task force to address it.

But as we look at the budget shortages, as we look at prioritization in the context of perhaps the budgets will even get worse down the road, this is one where it is very difficult to find the resources to put on it.

Senator KLOBUCHAR. I understand that. That is why I figured one thing we could do that would be helpful is to put some requirements in place—some States have—on the sale of these things so it is easier for local law enforcement to track. So I wanted to put the words in because you have a lot on your plate, and I think the best thing would be to make it a little easier for locals to handle this.

I had some questions, and I know Senator Kohl got into the economic espionage issue, which I think is critically important. We have many big companies in Minnesota that own many patents. My favorite statistic is that 3M has as many employees as they have inventions. There is one invention for each employee. And so we care very much about this espionage, especially over the Internet and some of the cyber crime that is going on. So I appreciate the work you are doing in this area and the way that you are adjusting to the ever changing technological climate with the FBI.

Thank you very much.

Mr. MUELLER. Thank you.

Senator WHITEHOUSE. [Presiding.] Welcome, Director Mueller. Good to see you.

Let me follow up on Senator Klobuchar's last point on our cyber vulnerability. Let me preface our remarks by saying that from my viewpoint on the Intelligence Committee, from my viewpoint on this Committee, from going out and seeing your folks in action at NCIJTF, from looking at some of the cases that have been put together, I am very impressed with the ability and the dedication of the forces that you have deployed against our cyber threat.

What I am concerned about is not their ability. It is their adequacy. It is the quantity, not the quality. I think you run some very, very high-quality folks, and I appreciate that.

I went out on a limb about two years ago and said that I thought that the theft of American intellectual property across our cyber networks was the biggest transfer of wealth in the history of the human species through theft and piracy and that we were on the losing end of it and we were not taking enough action to defend against it. And since then, General Alexander has said virtually the same thing. He is the head of Cyber Command and the head of NSA. And private sector observers like the latest McAfee report have again used almost the same language.

So here we are, assuming that to be true, on the losing end of the biggest transfer of wealth in the history of humankind, and I want to ask your continued support for my office's efforts to try to get a real understanding of what our FBI and DOJ resources are dedicated to this problem.

You have to really drill below the numbers, because I can ask DOJ and they can say, oh, well, there is a cyber person dedicated in every U.S. Attorney's Office, and I know perfectly well from having been a U.S. Attorney that that person may very well be doing no cyber cases at all. They may simply be the designee who puts the conference call on mute while they are doing other work.

So just that number does not really help, and so we are trying to work through who is really on this cyber problem and how within the FBI. Are there people who are designated in your local offices who are in the same mode when there is a conference call to be had, they are the ones who take it but their workload is really elsewhere? Are there folks whose role is really sort of forensic clean-up, the people who, you know, when you raid a place, they grab the computers and they do the download? That is all important stuff, but it is not really the cyber battle.

One of the things that I am concerned about is that when you look at the metrics of cases that are produced, again, I see some great cases, but I do not see a ton of them. In terms of beating down the botnets that attack our systems through denial of service attacks, you guys helped, I think, both take down the Coreflood and the Rustock botnets. Those were a very big deal. The Rustock botnet made a really measurable dent in the amount of spam that is out there on the Internet. But there is still a ton of that stuff going on, and two great cases but it is not a lot of cases.

I am informed that if you look at intellectual property theft through cyber as the means, hacking into an American company's computer, accessing their confidential data, their formulas, their secrets, exfiltrating that out and then using that to compete against the company, we have made exactly zero cases; that in all of the cyber cases that we—all the intellectual property theft cases that we have made, there has been a human link. We have found the guy who is downloading it to a disk and putting it in his pocket.

My impression from my visit to the NCIJTF is that they are standing in front of a fire hose trying to do their very best to manage around just an immense amount of work. And from what I hear from private-sector folks, they would love to have more FBI and more federal law enforcement support when they have been hacked.

Now, nine times out of ten, they do not even know they have been hacked. They get told they have been hacked when your folks or Homeland Security come knocking on the door and say, "By the way, you might want to consider looking at this file."

But once they do know, having more support from you guys I think is—I think you are doing a great job with the resources you have, but I just feel that we are at a stage where this has become such a big problem, both as a national security problem to our electric grid, to our financial system, to our communications networks, if somebody decides to take those down, and as an industrial espio-

nage problem against our major competitive industries, and as a privacy problem. There is probably somebody in this room right now whose credit card and Social Security information is on some Estonian gangster's Web site for sale. There is just so much of it for sale right now.

And so there are all of these issues, and I feel that we need—in the same way that we had to move from just having a couple of aircraft in the U.S. Army years ago, we have got to have an Air Force on this one; that we need to be thinking about really what is the next step, how should we structure this. It is not enough just to add incrementally. We really need to kind of go “game on” on this.

So I would like your thoughts on that point. I know that OMB is a bit of a hazard for folks when you are being asked to argue beyond your allocated budget. But I would at least like to ask you to participate willingly and helpfully and continue to, because I have good support so far in trying to help work this through. We are trying to get something into the cyber bill that will at least put a structure into analyzing what our law enforcement posture should look like, how should it be resourced for the future. We have got a DEA. We have got an ATF. We have got a Secret Service. Maybe we should be thinking of building something that is equivalent for cyber as we look out.

What are your thoughts?

Mr. MUELLER. Let me start by saying I share your concern about putting the country and the Bureau in a posture to address this, and it is going to take a substantial reorientation of the Bureau to address this.

In terms of personnel—and one of the things that too often we do is we take pockets of the cyber issue and forget about them. And within the Bureau there are a number of initiatives we have undertaken over a period of time that fall within the cyber umbrella. Certainly the NCIJTF is one of them, and I think perhaps one of the most important of them. But, also, every one of our 56 field offices has cyber squads in which those individuals are doing cyber work.

Now, there are intrusions, and then there are cases—innocent images cases, quite obviously, that fall within that. But I would say that as we grow, the intrusions are perhaps more important. You hate to say that but, more importantly, need a different skill and need a different effort.

My discussions with our people are that we have to reorient the Bureau to address cyber in the same we reoriented the Bureau to address counterterrorism. That means beefing up our cyber squads and making them task forces, because you do not know where the cyber intrusion is going to occur, and you need to do the forensics in order to start the evaluation of attribution, much less the criminal case. And, consequently, it has to be distributed across the country, and the expertise has to be distributed across the country.

Now, it takes more of a headquarters role because, inevitably, in most of these, with it being botnet or what have you, you have victims in all the 50 States, and it may have started on Romania or Morocco or what have you. And, consequently, the old way of allocating responsibility to the office of origin or the first U.S. Attorney

who happens to get the subpoena in to the grand jury does not work in this environment. And so what we are working with in the Bureau is putting together a distributed——

Senator WHITEHOUSE. And if you do not mind me interjecting, plus in those cases you really do not have a criminal case. You have a civil effort to shut it off, which Rustock and Coreflood did brilliantly, but it is hard to sort of tee that up within the FBI's structure when there is no criminal case contemplated when you are——

Mr. MUELLER. Well, we look at it as national security—I mean, this is one of the problems that you have in cyber. At the time of the cyber intrusion, you do not know whether it is a state actor, you do not know whether it is organized crime or organized crime working for a state actor, or an individual or group of individuals who are not necessarily organized but distributed the anonymous type of attacks or, last, the 18-year-old who is particularly adept and wants to make his mark or her mark by intercepting. And so you cannot immediately put it into a cubbyhole of national security or this particular crime.

Consequently, NCIJTF with its 18 counterparts and with the distributed network, in my mind, gives us the ability to identify that intrusion, work on that intrusion with DHS protecting the infrastructure, but our gathering the information and helping on identifying the attribution for that particular tack.

I do believe that something like the Regional Computer Forensics Laboratories—yes, they do the exploitation, but it is the same expertise that you need to do the attribution in terms of a cyber attack. So we have got 16 of them. I would love to have more of those.

There are other aspects of the organization, the FBI organization, that have to be integrated. You can have cyber attacks that are undertaken by terrorists. It can be by state actors or espionage. And you need in both of those expertise as to who are the terrorists who would undertake it or who were the countries and the intelligence agencies of those countries who would undertake it. And, consequently, you have to merge the cyber expertise along with the substantive expertise in that particular area, and we are reorganizing to do that.

Bottom line, there is a long way to go for all of us, but it is a sharing of intelligence and developing the capability to take that intelligence and work with not only our persons in the United States but within NSA, CIA, and the others outside, which that will enable us to be successful in this particular arena.

Senator WHITEHOUSE. Good. Well, I really thank you for the excellent work that the Bureau is doing on this, and I look forward to working hard to make sure that you have got the resources as well that you need.

I will close by observing that these cases are immensely complicated and difficult. If you look at the complicating factors that make a case difficult, it has virtually all of them. It has probably the worst complicating factor of international domain and having to work through legats and having to work through treaties and having to work in foreign countries. It has the complicating factor of, as you pointed out, integration with our intelligence community

and having to deal with the security and classified nature of some of that and protecting sources and methods.

The cases themselves are challenging and difficult, as difficult as any RICO case can be. The forensics are very important, trying to figure out how this stuff actually works and be able to testify about it clearly. And then there is just a lot of work putting it together because some of these things are very big operations.

So when you combine all of that, each case could really be a huge vacuum for effort in order to succeed. So I think that is an important appreciation that I wanted to put into the record as we go about building this. This is not like buy-bust gun cases where you can knock them off, you know, one after another. These are the kinds of cases that could simply swamp a small U.S. Attorney's Office and present immense challenges.

Mr. MUELLER. Well, that is where we push resources, and we have to be far more flexible. We have to have virtual teams addressing these cases. Both of us have done RICOs. We could do RICOs. And these cases are complicated, but one thing that often is lost is there is a warm body behind that computer. And what you want to do is identify those individuals and arrest them and incarcerate them so that there is deterrence. You can talk about protecting the networks. You can talk about tracking the signature back to some particular country. But then there has to be action, and that is where our role comes in.

Senator WHITEHOUSE. Well, I appreciate it. I think I am the last person standing in this hearing, so I will call it to its conclusion. I thank you for coming up, as you have so often done, to face the oversight of this Committee. You always do so very professionally, and your organization is first rate. So we are always delighted to have you here.

The record will remain open for one additional week in case there is anything further that anybody wishes to submit. But the hearing is closed.

Mr. MUELLER. Thank you.

Senator WHITEHOUSE. Thank you.

[Whereupon, at 12:15 p.m., the Committee was adjourned.]

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

A P P E N D I X

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Witness List

Hearing before the
Senate Committee on the Judiciary

On

“Oversight of the Federal Bureau of Investigation”

Wednesday, May 16, 2012
Dirksen Senate Office Building, Room 226
10:00 a.m.

The Honorable Robert S. Mueller, III
Director
Federal Bureau of Investigation
United States Department of Justice
Washington, DC

PREPARED STATEMENT OF CHAIRMAN PATRICK LEAHY

**STATEMENT OF SENATOR PATRICK LEAHY (D-Vt.),
CHAIRMAN, SENATE JUDICIARY COMMITTEE
HEARING ON OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION
MAY 16, 2012**

It is appropriate that we welcome Director Robert Mueller of the Federal Bureau of Investigation back to the Committee during National Police Week. Yesterday I attended the National Peace Officers' Memorial Service with President Obama at the Capitol. Every year we lose too many fine law enforcement officers in the line of duty. I know Director Mueller is keenly aware of their sacrifice and is focused as I am on how best to protect those who protect us. I thank him and the hardworking men and women of the FBI who do vital work every day to keep us safe.

In the years since September 11th, the FBI has played an increasingly important role in our Nation's counterterrorism and intelligence gathering efforts. Together with prosecutors, other law enforcement partners, and the intelligence community, the FBI has helped obtain hundreds of terrorism convictions in our federal criminal courts.

Earlier this month, a federal jury in New York handed down a guilty verdict in one of the most serious terrorism plots since 9/11, which involved plans to carry out suicide bombings in the New York subway in 2009. Contrary to the fearful predictions of some, this major terrorism trial proceeded without a hitch in a federal court in the heart of New York City. There was hardly any disruption of the lives of New Yorkers who live and work near the courthouse.

The defendant was convicted without the need for mandatory military custody or interrogation, and certainly without the need for indefinite detention at Guantanamo Bay or elsewhere. He will be sentenced later this year, and faces life imprisonment. This is only the latest example of federal law enforcement, prosecutors, and criminal courts successfully investigating and trying terrorism cases. In recent years, the Christmas Day bomber and the Times Square bomber were convicted and sentenced to life imprisonment after the FBI used its expertise and experience to obtain Mirandized statements, without resorting to torture.

In contrast, the military commissions proceedings against the 9/11 plotters are just beginning at Guantanamo Bay. There will undoubtedly be lengthy litigation concerning the torture and mistreatment of certain defendants, and the trial itself will not start until sometime next year. Moreover, as Director Mueller pointed out last year during the debate over the defense authorization bill, mandating military custody in these situations merely hampers the FBI's ability to react swiftly and flexibly in gathering intelligence and evidence. That is one of the reasons why I have joined Senator Mark Udall in cosponsoring the Due Process and Military Detention Amendments Act, which would repeal that mandatory military detention requirement.

In the coming months, I also look forward to speaking with the Director about the administration's request for reauthorization of the FISA Amendments Act. I certainly appreciate the importance of providing the intelligence community with appropriate surveillance tools to help protect our country against terrorist threats. But we must also be sure that we are conducting sufficient oversight to ensure that we protect the privacy rights and civil liberties of law-abiding Americans. That is what I tried to do when we reauthorized certain provisions of

the USA PATRIOT Act, and I am disappointed that commonsense, bipartisan improvements were ultimately not enacted. As Congress considers the administration's request to reauthorize the FISA Amendments Act, I intend to look at whether we need to strengthen accountability, privacy, and civil liberties protections in the various parts of FISA.

While faced with daunting national security challenges, Director Mueller has also ensured that the FBI has maintained its historic focus on fighting crime. At a time of economic crisis and shrinking state and local law enforcement budgets, many expected violent crime to skyrocket. Instead, crime rates across the country have continued to decline. Along with the commitment of the President and the Congress to continued federal assistance to state and local law enforcement, the dedicated service of FBI agents throughout the country has played an important role in helping to keep crime rates low and Americans safe in their communities.

The FBI and the Justice Department have also worked hand in hand with us to make great strides toward more effective fraud prevention and enforcement. In the last Congress, I worked hard with Senators on both sides of the aisle to craft and pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade. We enacted important anti-fraud provisions as well as part of both the Affordable Care Act and Wall Street reform legislation. I am pleased to see that the FBI has greatly increased the number of agents investigating fraud. These new agents and new laws, together with hard work and effective investigative tactics, have led to record fraud recoveries and increased fraud arrests and convictions.

I commend the FBI for also continuing to combat corruption. We should pass commonsense, bipartisan legislation like the Fighting Fraud to Protect Taxpayers Act and the Public Corruption Prosecution Improvements Act to give the FBI more tools for fighting the scourges of fraud and corruption that have shaken the faith of the American people in recent years.

I thank the Director, again, for continuing to serve the American people and welcome him back to the Committee.

#####

PREPARED STATEMENT OF HON. ROBERT S. MUELLER, III



Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

MAY 16, 2012

**Statement for the Record
Robert S. Mueller, III
Director
Federal Bureau of Investigation**

**Committee on the Judiciary
United States Senate**

**Oversight of the Federal Bureau of Investigation
May 16, 2012**

Good morning, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

As you know, the Bureau has undergone unprecedented transformation in recent years. Since the attacks of September 11th, we have refocused our efforts to address and prevent emerging terrorist threats. The terrorist threat is more diverse than it was 10 years ago, but today, we in the FBI are better prepared to meet that threat.

We still confront traditional espionage and work diligently to prevent foreign intelligence agents from gaining our nation's political, military or economic secrets.

We also face increasingly complex threats to our nation's cyber security. Nation-state actors, sophisticated organized crime groups, and hackers for hire are stealing intelligence and national security data, as well as trade secrets and valuable research from America's companies, universities, and government agencies. These cyber threats are also a risk for our nation's critical infrastructure.

Yet national security is not our only concern, as we remain committed to our criminal programs. In the economic arena, investment fraud, mortgage fraud, securities fraud and health care fraud have harmed the world's financial system and victimized investors, homeowners, and taxpayers.

And although crime rates may be down nationwide, gang violence still plagues many neighborhoods, and our communities continue to confront violent crime, crimes against children, and threats from transnational organized crime.

As national security and criminal threats continue to evolve, so too must the FBI change to counter those threats. We must continue to use intelligence and investigative techniques to find and stop criminals and terrorists before they act. As we face greater challenges, we in the Bureau are relying on our law enforcement and private sector partners more than ever before.

The FBI remains firmly committed to carrying out our mission while protecting the civil liberties of the citizens we serve.

Counterterrorism

Counterterrorism remains our top priority.

In the past decade, Al Qaeda has become decentralized, but the group remains committed to high-profile attacks against the West. We confirmed this with records seized from Osama bin Laden's compound just over a year ago, as well as the recent conviction of an Al Qaeda operative plotting to conduct coordinated suicide bombings in the New York City subway system.

Al Qaeda affiliates and adherents, especially Al Qaeda in the Arabian Peninsula (AQAP), currently represent the top counterterrorism threat to the nation. These groups have attempted several attacks in and on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

We also remain concerned about the threat from homegrown violent extremists. Over the last two years, we have seen increased activity among extremist individuals. These individuals have no typical profile; their experiences and motives are often distinct. But they are increasingly savvy and willing to act alone, which makes them difficult to find and to stop.

For example, in February 2012, the FBI arrested Amine El Khalifi, a 29-year-old Moroccan immigrant, for allegedly attempting to detonate a bomb in a suicide attack on the U.S. Capitol. According to court documents, Khalifi believed he was conducting the terrorist attack on behalf of al Qaeda, although he was not directly affiliated with any group.

Another example is the case of Rezwan Ferdaus, a 26-year-old U.S. citizen and graduate student residing in Ashland, Massachusetts. Last fall, Ferdaus allegedly planned to use unmanned, remote-controlled aircraft to attack locations in Washington, D.C., including the U.S. Capitol and the Pentagon. Ferdaus was influenced by radical websites advocating violent extremism, among other things, and had expressed admiration for Al Qaeda's leaders, but was not directly affiliated with any group. He had allegedly become extremist on his own, making his activities much more difficult to detect. Ferdaus is currently awaiting trial in the United States District Court for the District of Massachusetts.

Much like every other multi-national organization, terrorist groups are using the Internet to grow their business and to connect with like-minded individuals. Al Qaeda uses online chat rooms and web sites to recruit and radicalize followers to commit acts of terrorism. AQAP has produced a full-color, English language online magazine. Cases such as these illustrate why we in the Intelligence Community must continue to enhance our intelligence capabilities and to share information to ensure that critical information gets to the right people – before any harm is done. The FISA Amendments Act (FAA), allows the Intelligence Community to collect vital

information about international terrorists and other important targets overseas while providing a robust protection for the civil liberties and privacy of Americans. I join the Attorney General and the Director of National Intelligence in urging Congress to reauthorize this authority before it expires at the end of this year.

The Bureau itself has established a Countering Violent Extremism (CVE) Office within the National Security Branch (NSB) to improve our effectiveness in empowering our state, local, and community partners to assist in this effort. The duties and goals of this office include developing a better understanding of, and countering the threat of, violent extremism in the United States, strengthening community partnerships and providing to state and local officials and to community leaders unclassified briefings regarding the threat of extremism, addressing CVE-related operational and mission-support needs, including investigations, analysis, and training, and coordinating Bureau interests with regard to CVE matters with those of other agencies to ensure U.S. Government efforts are aligned.

Counterintelligence

We still confront traditional espionage – spies working under diplomatic cover, or even posing as ordinary citizens.

Today’s spies are also students, researchers, businesspeople, or operators of “front companies.” And they seek not only state secrets, but trade secrets, research and development, intellectual property, and insider information from the federal government, U.S. corporations, and American universities.

Consider the recent case of Stewart David Nozette, a scientist who once worked for the Department of Energy, the Department of Defense, NASA, and the National Space Council. He was sentenced in March to 13 years in prison for attempted espionage, conspiracy to defraud the United States, and tax evasion after providing classified information to an undercover FBI agent whom he believed to be an Israeli intelligence officer.

In another case, Hanjuan Jin, a former software engineer at Motorola, Inc., was found guilty in February on charges of stealing the company’s trade secrets. She was stopped by U.S. customs officials in February 2007 at Chicago’s O’Hare International Airport with more than 1,000 electronic and paper proprietary documents from Motorola. She was attempting to travel on a one-way ticket to China. Authorities also recovered multiple classified Chinese military documents that described telecommunication projects for the Chinese military.

In another case, 36-year DuPont employee, Tze Chao, pled guilty in March to providing trade secrets concerning DuPont’s proprietary titanium dioxide manufacturing process to companies controlled by the Chinese government. He admitted providing information he understood to be secret to DuPont and not available to the public. He faces up to 15 years in prison and a \$500,000 fine plus restitution.

These cases illustrate the growing scope of the “insider threat” — when employees use their legitimate access to steal secrets for the benefit of another company or country.

Cyber

The counterintelligence threat is quickly becoming cyber-based. So much sensitive data is stored on computer networks, our adversaries often find it as effective, or even more effective, to steal vital strategic and economic information through cyber intrusions, rather than through more traditional human spies.

The cyber threat has evolved significantly over the past decade. Indeed, we anticipate that cyber security may become our highest priority in the future.

Foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate important government and military information, as well as valuable commercial data — information that can compromise national security as well as improve the competitive advantage of state-owned companies.

Unlike state-sponsored intruders, hackers for profit do not seek information for political power; rather they seek information for sale to the highest bidder. Some of these once-isolated hackers have joined forces to create criminal syndicates. Organized crime in cyber space offers a higher profit with a lower probability of being identified and prosecuted.

Additionally, hackers and hacktivist groups such as Anonymous and Lulz-Sec are pioneering their own forms of digital anarchy.

The end result of these developments is that we are losing data, money, ideas, and innovation. And as citizens, we are increasingly vulnerable to losing our personal information.

We in the FBI have built up an expertise to address these threats, both here at home and abroad.

We have approximately 70 cyber squads across our 56 field offices, with more than 1,000 specially trained agents, analysts, and forensic specialists. The FBI also has 63 Legal Attaché offices that cover the globe. Together with our international counterparts, we are sharing information and coordinating investigations. We have Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players.

Here at home, the National Cyber Investigative Joint Task Force brings together 20 law enforcement, military, and intelligence agencies to investigate current and predict future attacks. With our partners at DOD, DHS, CIA, and the NSA, we are targeting the cyber threats that face

our nation. The Task Force operates through Threat Focus Cells – specialized groups of agents, officers, and analysts that are focused on particular threats, such as botnets.

Together with our intelligence community and law enforcement agency partners, we are making progress toward defeating the threat – through our use of human sources, technical surveillance, and computer science.

Last April, with our private sector and law enforcement partners, the FBI dismantled the Coreflood botnet. This botnet infected an estimated two million computers with malware that enabled hackers to seize control of the privately owned computers to steal personal and financial information.

With court approval, the FBI seized domain names and re-routed the botnet to FBI-controlled servers. The servers directed the zombie computers to stop the Coreflood software, preventing potential harm to hundreds of thousands of users.

In another case, last fall we worked with NASA’s Inspector General and our partners in Estonia, Denmark, Germany, and the Netherlands to shut down a criminal network operated by an Estonian company by the name of Rove Digital.

The investigation, called Operation Ghost Click, targeted a ring of criminals who manipulated Internet “click” advertising. They redirected users from legitimate advertising sites to their own advertisements and generated more than \$14 million in illegal fees. This “click” scheme impacted more than 100 countries and infected four million computers, half a million of which were here in the United States.

We seized and disabled rogue servers, froze the defendants’ bank accounts, and replaced the rogue servers with legitimate ones to minimize service disruptions. With our Estonian partners, we arrested and charged six Estonian nationals for their participation in the scheme.

Together with our partners at DHS and the National Cyber-Forensics Training Alliance, we are using intelligence to create an operational picture of the cyber threat to identify patterns and players, to link cases and criminals.

We must continue to share information with our partners in law enforcement, in the Intelligence Community, and in the private sector.

We also must segregate mission-centric data from routine information. We must incorporate layers of protection and layers of access to critical information. And when there is a compromise, we must limit the data that can be gleaned from it.

•

Attribution is critical to determining whether an attack on a U.S. company is perpetrated by a state actor, an organized criminal group or a teenage hacker down the block. We can use the ability to attribute an attack to a specific attacker to help deter future attacks.

We cannot simply minimize vulnerabilities and deal with the consequences. Collectively, we can improve cyber security and lower costs with systems designed to catch threat actors, rather than simply to withstand them.

Financial Crimes

We have witnessed an increase in financial fraud in recent years, including mortgage fraud, health care fraud, and securities fraud.

Mortgage Fraud

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. At the end of last year, the FBI had nearly 2,600 mortgage fraud investigations nationwide — and a majority, over 70 percent, of these cases included losses greater than \$1 million dollars.

With the collapse of the housing market, we have seen an increase in schemes aimed at distressed homeowners, such as loan modification scams and phony foreclosure rescues. So-called “rescue services” claim they can expose errors by lenders that might allow owners to keep their homes. In reality, they are just a clever way to lure nervous consumers into giving up sensitive personal information and paying thousands of dollars in fees for false hopes. Indeed, in some cases, these criminals convince homeowners to sign away the deeds to their homes.

Other criminals preyed on investors’ hopes of cashing in before the housing bubble burst. In March, 61-year-old Andrew Williams, Jr., of Hollywood, Florida, was sentenced to 150 years in prison for his role in a \$78 million mortgage fraud scheme. Through the scheme, Williams promised to pay off homeowners’ mortgages in five to seven years following an initial investment of \$55,000. Unfortunately for investors, this was no more than a Ponzi scheme. Those who paid the fee and joined the “Dream Homes Program” later found that there was no money left to fund their mortgage payments.

The FBI has made mortgage fraud a top priority, because we recognize its negative impact on homeowners, neighborhoods, and our nation’s economy.

Over the past four years, we have nearly tripled the number of Special Agents investigating mortgage fraud. Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud.

We also work closely with the Department of Housing and Urban Development's Office of Inspector General, U.S. Postal Inspectors, the IRS, the FDIC, SIGTARP, the U.S. Trustee Program, the Federal Housing Finance Agency's Office of Inspector General, the Federal Trade Commission, and the Secret Service, as well as with state and local law enforcement offices.

Health Care Fraud

Health care spending currently makes up about 18 percent of our nation's total economy and continues to rise. These large amounts of money present an attractive target for criminals — so much so that we lose tens of billions of dollars each year to health care fraud.

In February, the Medicare Fraud Strike Force — a partnership between the Department of Justice and the Department of Health and Human Services — broke up the largest alleged home health care fraud scheme ever committed.

Dr. Jacques Roy, the owner of Medistat Group Associates in the Dallas area, was arrested along with several others for allegedly billing nearly \$375 million in fraudulent Medicare and Medicaid claims for home health care services. Between January 2006 and November 2011, Medistat had more purported patients than any other medical practice in the United States — including more than 11,000 patients from more than 500 home health agencies.

Since their inception in March 2007, Medicare Fraud Strike Force operations have charged more than 1,300 individuals who collectively have falsely billed the Medicare program for more than \$4 billion. Recently, a nationwide takedown by Medicare Fraud Strike Force operations in seven cities resulted in charges against 107 individuals, including doctors, nurses and other licensed medical professionals, for their alleged participation in Medicare fraud schemes involving approximately \$452 million in false billing.

Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, and every taxpayer who funds Medicare, is a victim.

As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used to care for the sick — not to line the pockets of criminals.

Corporate and Securities Fraud

Another area where our investigations have increased substantially in recent years is in corporate and securities fraud. Since September 2008, we have seen a 49 percent increase in these cases to more than 2,600 today.

One of our largest insider trading cases centered on the Galleon Group, a \$7 billion dollar hedge fund based in New York. Using evidence obtained through court-approved wiretaps,

attorneys and corporate insiders at several Fortune 500 companies were convicted of leaking proprietary information. The owner of the Galleon Group was convicted of multiple counts of securities fraud and sentenced in October to 11 years in prison — the longest sentence ever for insider trading. And in March 2012, Allen Stanford, former chairman of the board of Stanford International Bank, was convicted on wire, mail and other fraud charges for orchestrating a \$7 billion investment fraud scheme.

As financial crimes such as these become more sophisticated, so too must the FBI. In addition to devoting more agents and analysts, we established a Forensic Accountant Program three years ago. Under this program we have hired nearly 250 forensic accountants who are trained to catch financial criminals.

Three years ago, we also established the FBI's Financial Intelligence Center to strengthen our financial intelligence collection and analysis. The Center coordinates with FBI field offices to complement their resources and to identify emerging economic threats.

In 2010, the FBI began embedding Special Agents at the SEC, which allows us to see tips about securities fraud as they come into the SEC's complaint center. This, in turn, enables us to identify fraud trends more quickly and to push intelligence to our field offices so that they can begin criminal investigations where appropriate.

Gangs/Violent Crime

The most recent Uniform Crime Report (UCR) indicates violent crime continues to fall. However, for some cities and towns across the nation, violent crime — including gang activity — continues to pose a real problem.

Gangs have become more sophisticated. They have expanded their operations from street violence and drug trafficking to alien smuggling, identity theft, and mortgage fraud. Our Violent Crime, Violent Gang/Safe Streets, and Safe Trails Task Forces target major groups operating as criminal enterprises — high-level groups engaged in patterns of racketeering. This allows us to identify senior leadership and to develop enterprise-based prosecutions.

The FBI is also working to ensure crimes are being reported accurately. In collaboration with our state and local partners, the UCR program recently adopted a new, more inclusive definition of rape, which more accurately reflects current state laws defining the crime. This change will provide better data for our law enforcement partners in their efforts to respond to violent crimes. The Bureau is also beginning to look for ways to increase the accuracy and utility of the UCR more generally. These plans include collaborating within DOJ and the law enforcement community to increase the usage of the National Incident Based Reporting System (NIBRS) which is part of the UCR. Increased coverage of incident based reporting will lead to a more detailed and meaningful picture of crime in America.

Transnational Organized Crime

We also continue to confront organized crime. Crime syndicates run multi-national, multi-billion-dollar schemes – from human trafficking to health care fraud, and from computer intrusions to intellectual property theft.

These sophisticated enterprises operate both overseas and in the United States, and include Russian, Asian, Italian, Balkan, Middle Eastern, and African syndicates as well as Outlaw Motorcycle Gangs.

In the fall of 2010, an investigation by the FBI and its partners led to the indictment and arrest of more than 70 members and associates of an Armenian organized crime ring for their role in nearly \$170 million in fraudulent Medicare billings. This case included more than 160 phony medical clinics. Some of the subjects opened bank accounts to receive Medicare funds and submitted applications to Medicare to become Medicare providers.

The annual cost of transnational organized crime to the U.S. economy is estimated to be in the tens of billions of dollars. The effects of these schemes filter down to everyday Americans, who pay more for gas, health care, mortgages, clothes and food, not to mention the economic and social harm that such criminal activity costs our nation as a whole.

But organized crime does more than just impact our economy. These groups have the potential to infiltrate our businesses, and provide support to hostile foreign powers.

The FBI has squads dedicated to Eurasian Organized Crime investigations, including in New York, San Francisco, Miami, Philadelphia, Newark, and Chicago. Over the past decade, Asian criminal enterprises have evolved into transnational and decentralized networks that focus on low-risk and high-profit crimes. Chinese and Korean criminal networks across the United States obtain, sell, and use fraudulent U.S. identification documents to conduct a variety of financial crimes. The FBI is currently expanding its focus to include West African and Southeast Asian organized crime groups. The Bureau continues to share intelligence about criminal groups with our federal and international partners, and to combine resources and expertise to gain a full understanding of each group. In furtherance of these efforts, the FBI participates in the International Organized Crime Intelligence Operations Center. This center is responsible for coordinating the efforts of nine federal law enforcement agencies in combating non-drug transnational organized crime networks. The FBI is also enhancing its ability to address transnational criminal enterprises that operate along the Southwest Border and the Caribbean. We have developed Hybrid Squads to target these groups, which linked to U.S.-based gangs, cross-border drug trafficking, public corruption, money laundering, and violent crime.

No one department, agency, or country can fight organized crime on its own – we must work with our partners to end this predatory environment. We will continue to use all of our investigative tools, intelligence from our sources, and the strength of our partnerships to stop organized crime in the United States.

Crimes Against Children

The FBI remains vigilant in its efforts to keep children safe and to find and stop child predators. Through our partnerships with state, local, tribal, and international law enforcement, we are able to investigate crimes that cross geographical and jurisdictional boundaries. We are also able to share intelligence, resources, and specialized skills to prevent child abductions.

Through our Child Abduction Rapid Deployment Teams, the Innocence Lost National Initiative, the Office of Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to make the world a safer place for our children.

Last month we added accused child pornographer Eric Justin Toth to the FBI's Ten Most Wanted Fugitive list. Toth, who also goes by the name David Bussone, is a former private-school teacher and camp counselor who taught here in Washington, D.C. He has been on the run since 2008, after an FBI investigation revealed pornographic images on a camera in his possession while at the D.C. private school. There is a reward of up to \$100,000 for information leading directly to Toth's arrest.

Since its creation in 1950, the Top Ten list has been invaluable to the FBI, helping us to capture some of the nation's most dangerous criminals. Of the 495 fugitives named to the list, 465 have been apprehended or located. That level of success would not have been possible without the strong support of the public, which has helped capture 153 of the Top Ten fugitives.

Indian Country

The FBI also maintains primary federal law enforcement authority to investigate felony crimes on more than 200 Indian reservations nationwide. Last year, the FBI handled approximately 2,900 Indian Country investigations.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations concern homicide, crimes against children, or felony assaults. To address these threats, the FBI is deploying six new investigators to Indian Country as part of the Department of Justice's broader effort to fight crime in tribal communities.

The FBI continues to work with tribes through the Tribal Law & Order Act to help tribal governments better address the unique public safety challenges and disproportionately high rates of violence and victimization in tribal communities. The Act encourages the hiring of additional law enforcement officers for Indian lands, enhances tribal authority to prosecute and punish criminals, and provides the Bureau of Indian Affairs and tribal police officers with greater access to law enforcement databases.

The gang threat on Indian reservations also poses a concern for the FBI. Currently, the FBI has 15 Safe Trails Task Forces focused on drugs, gangs, and violent crimes in Indian Country. In addition, the FBI continues its efforts to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts.

We are using technology to improve the way we collect, analyze, and share information. In 2011, we debuted new technology for the FBI's Next Generation Identification System, which enables us to process fingerprint transactions much faster and with increased accuracy. We are also integrating isolated data sets throughout the Bureau, so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

Sentinel, the FBI's new information and case management program, will replace the outdated Automated Case Support System. Sentinel is transforming the way the FBI does business by moving the Bureau from a primarily paper-based case management system to an electronic workflow-based management system of records. The system's indexing ability will allow users to extract names, dates, vehicles, addresses, and other details, and to more efficiently share data with our law enforcement partners.

We expect that Sentinel will be deployed to the field by the end of this fiscal year, encompass all of its original design concept functionality and come in at budget or below.

Going Dark

As technology advances, both at the FBI and throughout the nation, we must ensure that our ability to obtain communications pursuant to court order is not eroded. The increasingly mobile, complex, and varied nature of communication has created a growing challenge to our ability to conduct court-ordered electronic surveillance of criminals and terrorists. Many communications providers are not required to build or maintain intercept capabilities in their ever-changing networks. As a result, they are too often not equipped to respond to information sought pursuant to a lawful court order.

Because of this gap between technology and the law, law enforcement is increasingly challenged in accessing the information it needs to protect public safety and the evidence it needs to bring criminals to justice. It is only by working together – within the law enforcement and intelligence communities, and with our private sector partners – that we will find a long-term solution to this growing problem. We must ensure that the laws by which we operate keep pace with new threats and new technology.

Civil Liberties/Rule of Law

Technology is one tool we use to stay one step ahead of those who would do us harm. Yet as we evolve and update our investigative techniques and use of technology to keep pace with today's complex threat environment, we always act within the confines of the rule of law and the safeguards guaranteed by the Constitution. The world around us continues to change, but our values must never change. Every FBI employee takes an oath promising to uphold the rule of law and the United States Constitution. I emphasize that it is not enough to catch the criminal; we must do so while upholding civil rights. It is not enough to stop the terrorist; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights – these are not our burdens. These are what make all of us safer and stronger. In the end, we will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

Conclusion

Chairman Leahy and Ranking Member Grassley, I thank you for this opportunity to discuss the FBI's priorities and state of the Bureau as it stands today. Mister Chairman, let me again acknowledge the leadership that you and this Committee have provided to the FBI. The transformation the FBI has achieved over the past 10 years would not have been possible without the support of Congress and the American people. I would be happy to answer any questions that you may have.

QUESTIONS

Questions for the Record for FBI Director Robert Mueller
Chairman Patrick Leahy
May 23, 2012

NCTC

1. In March, the Attorney General and the Director of National Intelligence released new guidelines governing the acquisition and retention of data by the National Counterterrorism Center (NCTC). Under these new guidelines, the NCTC now could retain vast amounts of data regarding U.S. persons for up to 5 years – well beyond the six months that was allowed under the previous guidelines. Five years seems like a long time to be retaining and sifting through data about U.S. persons who may have no connection whatsoever to terrorism.
 - A. As the FBI could be one of the agencies sharing datasets of information with the NCTC, do you agree that such vast amounts of data should be retained for up to five years?
 - B. What privacy laws, criteria, and factors will you consider in determining the length of time that the FBI will permit NCTC to retain the Bureau's data?

Unsolved Civil Rights Crimes

2. In 2008, President Bush signed the Emmitt Till Unsolved Civil Rights Crimes Act, a law I cosponsored here in the Senate and that Congressman John Lewis championed in the House. The law provides critical tools and resources for the Department of Justice and FBI to expeditiously investigate and prosecute decades-old unsolved civil rights crimes.

Two years ago, the FBI announced that it had closed all but a few unsolved civil rights cases. Because these decisions were not made publicly, many of those affected by these cases are left wondering how the decision to close them came about. There have also been questions as to how the remaining cases are being investigated and whether resources are being effectively allocated for localities to work with the FBI. There is some urgency since these cases are time-consuming to investigate, and the law sunsets in 2017.

 - A. How was the decision made to close some of these cases?
 - B. What resources has the FBI dedicated to the remaining cases?
 - C. How is the FBI working with local law enforcement on these investigations?

#

“Oversight of the Federal Bureau of Investigation”

May 16, 2012

Question from Senator Charles E. Schumer

I. Child Protection Improvements Act.

Currently, there is not one all-encompassing background check database available in this country that child service organizations can easily access to ensure they are not hiring criminals or sexual predators.

Oftentimes, individual states are the gatekeepers of criminal history information and can decide who has access to the FBI's background check information. In fact, 34 states do not have programs that would enable child service organizations to access the FBI's background check information.

The Child Protection Improvements Act would ensure that all youth-serving organizations will have access to the fingerprint-based criminal record checks of the F.B.I. database in a timely and affordable manner, so that criminals are not unknowingly employed in jobs that bring them in close contact with children.

Do you support this legislation, and do you think that Congress should act to pass this legislation as soon as possible?

Senate Committee on the Judiciary
Hearing on Oversight of the Federal Bureau of Investigation
May 16, 2011
Questions for the Record from Senator Charles Grassley
To Robert Mueller III
Director, Federal Bureau of Investigation

(1) National Security Leaks

Leaks of classified information to the media continue to plague critical intelligence and national security operations. It was recently reported that sources inside the government provided critical information about the role the intelligence community played in disrupting a plot to use a device similar to the Christmas Day bomber's "underwear bomb". At the hearing you stated that the FBI had "initiated an investigation into this leak and also affirmed...that leaks such as this threaten ongoing operations."

I agree that the leaks are a grave threat to our national security and that they put operations, and international partnerships, at risk. Unfortunately, it has become all too common that major intelligence and national security successes are followed by significant leaks of classified information to the media. Just yesterday, it was reported that documents released by the Defense Department and CIA reveal that the Administration leaked classified information to filmmakers that were preparing a film on the raid that killed Osama bin Laden.

- (a) When does the FBI anticipate completing the leak investigation into the information released about the operation that uncovered the new "underwear bomb"?
- (b) How much taxpayer money does a leak investigation of this nature cost the FBI?
- (c) How many agents are assigned to this investigation?
- (d) Has the FBI initiated an investigation into leaks to the filmmakers that were provided classified information regarding the raid that killed Osama bin Laden? If not, why not? If so, when will that investigation be completed?

(2) Over-classification of Information

Following the last FBI Oversight hearing, I asked you a written question about the classification of documents labeled as "Sensitive Security Information". While your response noted that the FBI "erroneously" inserted language attempting to label the document as Sensitive Security Information under 49 CFR parts 15 and 1520, which provide authority to the Federal Highway Administration and Transportation Security Administration, it failed to answer my specific questions. Accordingly, provide responses to the following questions.

- (a) Why was the FBI utilizing classification authority under 49 CFR parts 15 and 1520?
- (b) Does the FBI authorize the Administrator of the Transportation Security Administration to declassify FBI documents?
- (c) Aside from this instance, has the FBI ever stamped a document under the authority under 49 CFR parts 15 and 1520? If so, how many times and why?

- (d) Does the FBI have a process aimed at identifying and verifying the classification of materials in order to prevent future mislabeling? For example, once labeled, is the designation ever proactively reviewed?

(3) FBI Crime Lab/DOJ Task Force

As we discussed at the hearing, a Department of Justice task force worked from 1996 to 2004 to examine potentially flawed forensic work in the FBI lab. According to press reports, the task force identified more than 250 convictions in which the lab's flawed forensic work was determined to be critical to the conviction. In some of those cases, the lab's work was so problematic that the task force had to complete a fresh scientific assessment.

When the task force wrapped up in 2004, it only notified prosecutors in the problem cases of its findings, rather than defendants. There has been no public disclosure of which prosecutors were notified of problems in which cases. In 2003, unnamed government sources were quoted as being aware that of the prosecutors contacted, only 100 to 150 actually notified the defendants in the cases.

Questions:

- (a) Why did the task force decide to notify only prosecutors instead of all parties in these cases?
- (b) What were the notification procedures?
- (c) Did the Justice Department share records with the FBI about what notifications went to the prosecutor?
- (d) Which prosecutors were notified?
- (e) Which defendants were actually notified?
- (f) Which defendants were not notified?
- (g) If press reports are correct, why were only 100 to 150 defendants notified?

(4) Mark Rossetti

On October 17, 2011 I wrote you a letter seeking information on Boston-area mobster Mark Rossetti. According to news reports, the FBI had a long-term relationship with Mr. Rossetti that was not disclosed to the Massachusetts State Police. It was only when the State Police wiretapped Mr. Rossetti and heard him speaking to his handler that they were able to confirm that he was an informant.

Based on the FBI's response and from meetings my staff has had with the FBI, I have been told that there is an ongoing inspection of the Boston FBI's actions. So far, this investigation has taken over six months.

Questions:

- (a) What is the status of this inspection?
- (b) When do you expect it to conclude?
- (c) When the inspection does conclude, will you send this committee its final report?
- (d) For this inspection, did the FBI interview former Massachusetts State Police Detective Bill McGreal?

(5) Murder Investigation of Border Patrol Agent Brian Terry

It's now been almost a full year and a half since FBI began the investigation into the shooting of Border Patrol Agent Brian Terry. However, the family of Agent Terry is still left wondering who shot their son. On October 20, 2011, I sent a letter along with House Oversight and Government Reform Committee Chairman Darrell Issa, but the Bureau's May 5, 2012 response did little to answer our questions.

Questions:

- (a) What time did the FBI arrive on the scene?
- (b) Which other state, local, or federal agencies were already present when the FBI arrived?
- (c) What time did the first ATF personnel arrive at the scene?
- (d) When and how were the trace requests for weapons recovered at the scene submitted to ATF?
- (e) Has the FBI submitted any other trace requests to ATF in connection with the Terry murder case? If so, please describe the circumstances in detail, providing the serial number and date of each request.
- (f) Has the FBI submitted any trace requests to ATF in any of its other cases where the gun was connected to Fast and Furious? If so, please describe the circumstances in detail, providing the serial number and date of each request.
- (g) How many of the suspects encountered by Agent Terry's Border Patrol unit are currently at large? What steps has the FBI taken to apprehend them and what is the status of the FBI's search?
- (h) Why has so much time passed without the shooter of Agent Terry being arrested?
- (i) Does the FBI know the identity of Agent Terry's shooter? If so, why is that person not on the FBI's most wanted list?
- (j) When is this investigation going to be wrapping up?
- (k) According to press reports, three illegal immigrants were taken into custody "near the scene of the shootout" but were later "cleared by federal authorities," released, and deported to Mexico. Please explain the circumstances of their arrest and why they were released.
- (l) Is the FBI investigating the circumstances of how the guns from Fast and Furious came into the possession of the people shooting at our Border Patrol agents that night?

(6) FBI Jet Use

An internal FBI audit from earlier this year recommended that the FBI monitor not only how many requests for aircraft support were denied, but for what reasons they were denied (Audit Report 12-21, March 2012, xiv).

Questions:

- (a) Has the FBI instituted this tracking system? If so, do you have information on how many operation requests are denied because of transporting personnel? If not, why not?

SENATOR LINDSEY GRAHAM
 QUESTIONS FOR THE RECORD
 FOR THE HONORABLE ROBERT S. MUELLER, III
 DIRECTOR, FEDERAL BUREAU OF INVESTIGATIONS
 U.S. SENATE COMMITTEE ON THE JUDICIARY
 MAY 9, 2012

The Fifth Amendment to the Constitution of the United States states in part: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia when in actual service in time of War or public danger."

- (a) What time period is required for presentment under the criminal justice model? Does this requirement vary based upon whether the accused is a citizen or non-citizen?
- (b) During presentment under the criminal justice model can a person classified as an enemy combatant become entitled to legal counsel? If not at presentment, then when?

Under *Miranda*'s public safety exception, officers may question a suspect in custody without first obtaining a waiver of his right to remain silent if they reasonably believe the suspect has information that would save a life, prevent serious injury, or neutralize a substantial threat to property.

- (a) How long can a terror suspect be held under the *Miranda* public safety exception before *Miranda* rights would be required? Does that requirement differ based upon whether the suspect is a citizen or non-citizen?
- (b) Do you agree that enemy combatants held under the law of war are not entitled to *Miranda* warnings or legal representation when interrogated for intelligence purposes?
- (c) Do you agree that in international terrorism cases time is of the essence but that it may take weeks or months to elicit intelligence from a captured combatant?

Do you agree with the argument made by some that the United States is not part of the battlefield in the War on Terror? If so, why do you agree? If not, why not?

RESPONSES FROM HON. ROBERT S. MUELLER, III

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the May 16, 2012, Hearing Before the
Senate Committee on the Judiciary
Regarding "Oversight of the FBI"**

Questions Posed by Chairman Leahy

NCTC

1. In March, the Attorney General and the Director of National Intelligence released new guidelines governing the acquisition and retention of data by the National Counterterrorism Center (NCTC). Under these new guidelines, the NCTC now could retain vast amounts of data regarding U.S. persons for up to 5 years – well beyond the six months that was allowed under the previous guidelines. Five years seems like a long time to be retaining and sifting through data about U.S. persons who may have no connection whatsoever to terrorism.

a. As the FBI could be one of the agencies sharing datasets of information with the NCTC, do you agree that such vast amounts of data should be retained for up to five years?

Response:

Congress designated the National Counterterrorism Center (NCTC) to serve as "the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism." (Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638, 3673 (2004), section 1021.)

Because it can take time for connections among people and activities to develop and to be assessed, the FBI believes it is important that the NCTC have adequate time to analyze the datasets it receives pursuant to the various authorities designed to ensure the sharing of terrorism and terrorism-related information.

b. What privacy laws, criteria, and factors will you consider in determining the length of time that the FBI will permit NCTC to retain the Bureau's data?

Response:

These responses are current as of 7/3/12

As discussed above, the NCTC is designated by statute to serve as “the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism,” and it receives information from the FBI pursuant to authorities designed to ensure the sharing of terrorism and terrorism-related information.

The NCTC may only retain FBI information about United States persons as permitted by guidelines issued by the Attorney General and the Director of National Intelligence pursuant to Executive Order 12333 (1981) and the recordkeeping requirements the NCTC has established with the National Archives. Beyond requiring compliance with those authorities and the Privacy Act, the FBI would consider the nature of the dataset involved, its connection to terrorism, the amount of U.S person information that may be included but has no connection with terrorism, the purpose for which the information was collected, and the safeguards imposed on the use and dissemination of the data.

Unsolved Civil Rights Crimes

2. In 2008, President Bush signed the Emmett Till Unsolved Civil Rights Crimes Act, a law I cosponsored here in the Senate and that Congressman John Lewis championed in the House. The law provides critical tools and resources for the Department of Justice and FBI to expeditiously investigate and prosecute decades-old unsolved civil rights crimes.

Two years ago, the FBI announced that it had closed all but a few unsolved civil rights cases. Because these decisions were not made publicly, many of those affected by these cases are left wondering how the decision to close them came about. There have also been questions as to how the remaining cases are being investigated and whether resources are being effectively allocated for localities to work with the FBI. There is some urgency since these cases are time-consuming to investigate, and the law sunsets in 2017.

a. How was the decision made to close some of these cases?

Response:

The Emmett Till Unsolved Civil Rights Crime Act of 2007 (Pub. L. 110-344, 122 Stat. 3934 (2008)) requires the Department of Justice (DOJ) to designate a Deputy Chief in the Civil Rights Division to coordinate the investigations and prosecutions of the open cases subject to the Act (the Act addresses violations of criminal civil rights statutes that occurred no later than 1969 and resulted in a death). These open cases are being reviewed by the Deputy Chief and by FBI Supervisory Special Agents to determine

These responses are current as of 7/3/12

whether the case includes any subjects who have not been prosecuted and who are still living. If so, the case is analyzed to assess whether all investigative leads have been covered and whether there is sufficient evidence to move forward. If it is determined that investigation has not, and will not, result in sufficient evidence to prosecute, the Deputy Chief prepares a letter summarizing the investigative findings. This letter is hand delivered to the victim's known next-of-kin. After confirmation that the letter was delivered, the Deputy Chief authorizes that the case be closed.

b. What resources has the FBI dedicated to the remaining cases?

Response:

An FBI case agent has been assigned to each case being investigated under the cold case initiative. In addition, the FBI has designated a Cold Case Program Manager at FBI Headquarters. This Program Manager works with the case agents and serves as liaison between the FBI Field Offices and DOJ's Deputy Chief. While the need for resources varies from case to case, the Cold Case Program Manager is responsible for ensuring that each case has the necessary investigative resources.

c. How is the FBI working with local law enforcement on these investigations?

Response:

The FBI will work jointly with local law enforcement authorities on these cases when there is sufficient evidence to move forward and prosecution at the state level is appropriate due to the absence of Federal jurisdiction.

Questions Posed by Senator Schumer

Child Protection Improvements Act

3. Currently, there is not one all-encompassing background check database available in this country that child service organizations can easily access to ensure they are not hiring criminals or sexual predators.

Oftentimes, individual states are the gatekeepers of criminal history information and can decide who has access to the FBI's background check information. In fact, 34 states do not have programs that would enable child service organizations to access the FBI's background check information.

The Child Protection Improvements Act would ensure that all youth-serving

These responses are current as of 7/3/12

organizations will have access to the fingerprint-based criminal record checks of the F.B.I. database in a timely and affordable manner, so that criminals are not unknowingly employed in jobs that bring them in close contact with children.

Do you support this legislation, and do you think that Congress should act to pass this legislation as soon as possible?

Response:

The FBI is always pleased to provide its views of proposed legislation to appropriate DOJ officials pursuant to the Department's role in assisting in the development of the Administration's position.

Questions Posed by Senator Grassley

National Security Leaks

4. Leaks of classified information to the media continue to plague critical intelligence and national security operations. It was recently reported that sources inside the government provided critical information about the role the intelligence community played in disrupting a plot to use a device similar to the Christmas Day bomber's "underwear bomb". At the hearing you stated that the FBI had "initiated an investigation into this leak and also affirmed...that leaks such as this threaten ongoing operations."

I agree that the leaks are a grave threat to our national security and that they put operations, and international partnerships, at risk. Unfortunately, it has become all too common that major intelligence and national security successes are followed by significant leaks of classified information to the media. Just yesterday, it was reported that documents released by the Defense Department and CIA reveal that the Administration leaked classified information to filmmakers that were preparing a film on the raid that killed Osama bin Laden.

a. When does the FBI anticipate completing the leak investigation into the information released about the operation that uncovered the new "underwear bomb"?

Response:

The FBI cannot anticipate when we will complete this investigation, but the investigation is ongoing and active.

b. How much taxpayer money does a leak investigation of this nature cost the FBI?

These responses are current as of 7/3/12

c. How many agents are assigned to this investigation?

d. Has the FBI initiated an investigation into leaks to the filmmakers that were provided classified information regarding the raid that killed Osama bin Laden? If not, why not? If so, when will that investigation be completed?

Response to subparts b through d:

Although investigative costs vary widely, the costs of media leak investigations are often in the hundreds of thousands of dollars. Longstanding DOJ policy generally precludes the FBI from commenting on the existence or status of ongoing investigations and from disclosing nonpublic information about such investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede an FBI investigation.

Over-Classification of Information

5. Following the last FBI Oversight hearing, I asked you a written question about the classification of documents labeled as "Sensitive Security Information". While your response noted that the FBI "erroneously" inserted language attempting to label the document as Sensitive Security Information under 49 CFR parts 15 and 1520, which provide authority to the Federal Highway Administration and Transportation Security Administration, it failed to answer my specific questions. Accordingly, provide responses to the following questions.

a. Why was the FBI utilizing classification authority under 49 CFR parts 15 and 1520?

b. Does the FBI authorize the Administrator of the Transportation Security Administration to declassify FBI documents?

c. Aside from this instance, has the FBI ever stamped a document under the authority under 49 CFR parts 15 and 1520? If so, how many times and why?

Response to subparts a through c:

As we answered in response to the Question for the Record arising from the December 14, 2011, oversight hearing, cover memos forwarding the FBI's Domestic Investigations and Operations Guide (DIOG) to the Hill erroneously contained a reference to 49 CFR parts 15 and 1520 and to the Department of Transportation (DOT). This information was

These responses are current as of 7/3/12

in a section of the memo that intended to alert the reader that the DIOG is sensitive and, as we noted in our previous response, the assertion of the DIOG's sensitivity was accurate, even though our citations to 49 CFR and DOT were not. As our prior response advised, "the Department of Transportation is not involved in establishing handling caveats for FBI materials." To the best of our knowledge, this is the only instance in which we have made this administrative error. As noted in our prior response, the handling caveat that is most clearly and overtly applicable to the DIOG appears on the cover of the DIOG, itself.

d. Does the FBI have a process aimed at identifying and verifying the classification of materials in order to prevent future mislabeling? For example, once labeled, is the designation ever proactively reviewed?

Response:

Executive Order 13526, "Classified National Security Information" (December 29, 2009), prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The FBI complies with that Executive Order.

As indicated both above and in our response to the December 2011 Question for the Record, the DIOG is properly labeled as sensitive.

FBI Crime Lab/DOJ Task Force

6. As we discussed at the hearing, a Department of Justice task force worked from 1996 to 2004 to examine potentially flawed forensic work in the FBI lab. According to press reports, the task force identified more than 250 convictions in which the lab's flawed forensic work was determined to be critical to the conviction. In some of those cases, the lab's work was so problematic that the task force had to complete a fresh scientific assessment.

When the task force wrapped up in 2004, it only notified prosecutors in the problem cases of its findings, rather than defendants. There has been no public disclosure of which prosecutors were notified of problems in which cases. In 2003, unnamed government sources were quoted as being aware that of the prosecutors contacted, only 100 to 150 actually notified the defendants in the cases.

a. Why did the task force decide to notify only prosecutors instead of all parties in these cases?

b. What were the notification procedures?

These responses are current as of 7/3/12

c. Did the Justice Department share records with the FBI about what notifications went to the prosecutor?

d. Which prosecutors were notified?

e. Which defendants were actually notified?

f. Which defendants were not notified?

g. If press reports are correct, why were only 100 to 150 defendants notified?

Response to subparts a through g:

It is the FBI's understanding that these questions were also posed to the Attorney General following this Committee's June 12, 2012 DOJ oversight hearing and will be answered in that context.

Mark Rossetti

7. On October 17, 2011 I wrote you a letter seeking information on Boston-area mobster Mark Rossetti. According to news reports, the FBI had a long-term relationship with Mr. Rossetti that was not disclosed to the Massachusetts State Police. It was only when the State Police wiretapped Mr. Rossetti and heard him speaking to his handler that they were able to confirm that he was an informant.

Based on the FBI's response and from meetings my staff has had with the FBI, I have been told that there is an ongoing inspection of the Boston FBI's actions. So far, this investigation has taken over six months.

a. What is the status of this inspection?

b. When do you expect it to conclude?

Response to subparts a and b:

Indictments charging Rossetti with breaking and entering, extortion, and conspiracy have been filed by the Massachusetts Attorney General's office. In addition, the Essex County District Attorney's office is investigating Rossetti for alleged illegal drug activity. Because documents from both offices may provide information not previously available to us, the FBI anticipates obtaining and reviewing them as part of the inspection.

c. When the inspection does conclude, will you send this committee its final report?

These responses are current as of 7/3/12

Response:

The FBI will be able to follow up with the Committee after the inspection has been completed.

d. For this inspection, did the FBI interview former Massachusetts State Police Detective Bill McGreal?

Response:

Yes.

Murder Investigation of Border Patrol Agent Brian Terry

8. It's now been almost a full year and a half since FBI began the investigation into the shooting of Border Patrol Agent Brian Terry. However, the family of Agent Terry is still left wondering who shot their son. On October 20, 2011, I sent a letter along with House Oversight and Government Reform Committee Chairman Darrell Issa, but the Bureau's May 5, 2012 response did little to answer our questions.

a. What time did the FBI arrive on the scene?

b. Which other state, local, or federal agencies were already present when the FBI arrived?

c. What time did the first ATF personnel arrive at the scene?

d. When and how were the trace requests for weapons recovered at the scene submitted to ATF?

e. Has the FBI submitted any other trace requests to ATF in connection with the Terry murder case? If so, please describe the circumstances in detail, providing the serial number and date of each request.

Response to subparts a through e:

There are criminal charges pending related to this matter and the investigation is continuing. Longstanding DOJ policy generally precludes the FBI from commenting on the status of ongoing investigations and from disclosing nonpublic information about such investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would

These responses are current as of 7/3/12

impede an FBI investigation.

f. Has the FBI submitted any trace requests to ATF in any of its other cases where the gun was connected to Fast and Furious? If so, please describe the circumstances in detail, providing the serial number and date of each request.

Response:

While the FBI has not historically needed to centrally collect the results of trace requests submitted to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), we are aware of one instance in which a gun involved in an FBI case was linked to the Fast and Furious operation.

In March 2011, the ATF and FBI conducted a joint operation that included subjects in both New Mexico and Texas. Both subjects were arrested and a search warrant was executed on the home of the Texas subject. The FBI seized a pistol during that search and submitted a trace request to the ATF. In June 2011 the ATF advised that the pistol was associated with the Fast and Furious operation. This case is still pending and longstanding DOJ policy generally precludes the FBI from commenting on the status of ongoing investigations and from disclosing nonpublic information about such investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede an FBI investigation.

The FBI is aware of no other trace requests involving guns connected to the Fast and Furious operation.

g. How many of the suspects encountered by Agent Terry's Border Patrol unit are currently at large? What steps has the FBI taken to apprehend them and what is the status of the FBI's search?

Response:

On July 9, 2012, an indictment charging five individuals involved in the death of U.S. Border Patrol Agent Brian Terry was unsealed and an FBI reward of up to \$1 million for information leading to the arrest of four fugitives was announced. According to the indictment, Manuel Osorio-Arellanes, Jesus Rosario Favela-Astorga, Ivan Soto-Barraza, Heraclio Osorio-Arellanes, and Lionel Portillo-Meza were charged with crimes including first degree murder, second degree murder, conspiracy to interfere with commerce by robbery, attempted interference with commerce by robbery, carrying and use of a firearm during a crime of violence, assault on a federal officer, and possession of a firearm by a

These responses are current as of 7/3/12

prohibited person. A sixth defendant, Rito Osorio-Arellanes, is charged only with conspiracy to interfere with commerce by robbery. Manuel Osorio-Arellanes has been in custody since his arrest on December 14, 2010, the night of the shooting. Rito Osorio-Arellanes has been in custody since December 12, 2010, when he was arrested by Border Patrol agents on immigration charges.

h. Why has so much time passed without the shooter of Agent Terry being arrested?

Response:

Longstanding DOJ policy generally precludes the FBI from commenting on the status of ongoing investigations and from disclosing nonpublic information about such investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede an FBI investigation.

i. Does the FBI know the identity of Agent Terry's shooter? If so, why is that person not on the FBI's most wanted list?

Response:

In order to be considered for inclusion on the FBI's "Ten Most Wanted" list, an individual must have a lengthy record of committing serious crimes and/or be considered a particularly dangerous menace to society due to the current criminal charges. The absence of a given person from the list does not mean a crime committed by that person is any less tragic or reprehensible than another crime, and it does not mean the FBI is any less dedicated to the investigation or committed to its successful resolution. While the FBI's "Top Ten Most Wanted" list is an important means of alerting the public to particularly dangerous fugitives, rewards (such as the FBI reward of up to \$1 million for information leading to the arrest of the four fugitives in the Terry murder, noted above) are also critical to obtaining the assistance of the public.

j. When is this investigation going to be wrapping up?

Response:

Longstanding DOJ policy generally precludes the FBI from commenting on the status of ongoing investigations and from disclosing nonpublic information about such investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result

These responses are current as of 7/3/12

in the destruction of evidence, witness tampering, or other activity that would impede an FBI investigation.

k. According to press reports, three illegal immigrants were taken into custody “near the scene of the shootout” but were later “cleared by federal authorities,” released, and deported to Mexico. Please explain the circumstances of their arrest and why they were released.

Response:

Three individuals were arrested approximately 2.5 miles from the location where Border Patrol Agent Brian Terry was murdered. Based upon examination of the evidence collected at the scene and interviews that included these three individuals, it was determined that these three individuals were not part of the group that murdered Agent Terry. After spending time in jail on immigration charges, they were returned to Mexico.

l. Is the FBI investigating the circumstances of how the guns from Fast and Furious came into the possession of the people shooting at our Border Patrol agents that night?

Response:

Longstanding DOJ policy generally precludes the FBI from commenting on the status of ongoing investigations and from disclosing nonpublic information about such investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede an FBI investigation.

FBI Jet Use

9. An internal FBI audit from earlier this year recommended that the FBI monitor not only how many requests for aircraft support were denied, but for what reasons they were denied (Audit Report 12-21, March 2012, xiv). Has the FBI instituted this tracking system? If so, do you have information on how many operation requests are denied because of transporting personnel? If not, why not?

Response:

The FBI tracks requests for aircraft support, including the purpose for which the aircraft is requested. We prioritize these requests, with operational use being the first priority and transportation requests receiving a lower priority. To date, there has been only one instance in which an operational request could not be accommodated due to a previously

These responses are current as of 7/3/12

scheduled transportation request. In that instance, an aircraft was requested for use in a contingency option as backup to an operation planned for later that day. The FBI had two aircraft capable of supporting the request, but one of the aircraft was undergoing maintenance while the other one was supporting an executive transportation mission on the west coast and could not be repositioned from that location in time to support the contingency option. The FBI chartered a plane from an independent company to support the contingency option, but that option was not exercised because the operational plan was executed without incident.

Questions Posed by Senator Graham

10. The Fifth Amendment to the Constitution of the United States states in part: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia when in actual service in time of War or public danger."

a. What time period is required for presentment under the criminal justice model? Does this requirement vary based upon whether the accused is a citizen or non-citizen?

Response:

We understand this question to be asking about the requirement that an accused be brought before a magistrate after arrest. Rule 5 of the Federal Rules of Criminal Procedure requires that a person under arrest be brought before a federal magistrate judge without unnecessary delay. This requirement does not depend on citizenship. What constitutes "unnecessary delay" is determined by all the facts and circumstances. For example, courts have found delays to be necessary or reasonable and not in violation of the Rule 5 requirement for promptness when needed to transport the defendant, obtain jurisdictional determinations, await the availability of the magistrate judge, or provide medical care for or address the intoxication of the defendant. The Rule 5 promptness requirement can be waived by the defendant if the waiver is knowing and voluntary. As a matter of practice, a defendant is typically brought before the magistrate judge on the day of arrest or within 24 hours thereafter.

b. During presentment under the criminal justice model can a person classified as an enemy combatant become entitled to legal counsel? If not at presentment, then when?

Response:

An accused is advised of his right to counsel at the time of his or her initial appearance in court. This right applies to any individual charged in the Federal criminal justice system

These responses are current as of 7/3/12

with a violation of the U.S. Code, regardless of any designation related to combatant status.

11. Under Miranda's public safety exception, officers may question a suspect in custody without first obtaining a waiver of his right to remain silent if they reasonably believe the suspect has information that would save a life, prevent serious injury, or neutralize a substantial threat to property.

a. How long can a terror suspect be held under the Miranda public safety exception before Miranda rights would be required? Does that requirement differ based upon whether the suspect is a citizen or non-citizen?

Response:

We understand this question to be asking how long a terror suspect may be questioned before *Miranda* rights must be provided, assuming that *Miranda* applies. In *New York v. Quarles*, 467 U.S. 649 (1984), the Supreme Court recognized a limited exception to *Miranda*, allowing custodial statements to be admitted into evidence if the unwarned interrogation was reasonably prompted by a concern for public safety. For example, an agent may ask questions about possible impending or coordinated terrorist attacks or plots; the existence, number, locations, and activities or intentions of accomplices who may be plotting attacks; and the location and nature of weapons being used. After all applicable public safety questions have been exhausted, providing *Miranda* warnings will afford the government the broadest range of options available to address the threat posed by the individual. The length of public safety questioning is determined by the facts and circumstances of the case and the use of the exception does not depend upon citizenship.

b. Do you agree that enemy combatants held under the law of war are not entitled to Miranda warnings or legal representation when interrogated for intelligence purposes?

Response:

Absent a court order, foreign nationals captured overseas as enemy belligerents and maintained in Department of Defense (DoD) custody or effective control may not be provided *Miranda* warnings. (Pub. L. 111-84, Division A, Title X, Subtitle D, § 1040, 123 Stat. 2189, 2454 (2009).) In addition, pursuant to the Military Commissions Act, the accused in military commission proceedings under the Act need not receive *Miranda* warnings in order for their statements to be admitted as evidence in those proceedings. (10 U.S.C. §§ 948r(c) and (d).) If, however, the detainee might be prosecuted in an Article III court, the provision of *Miranda* warnings prior to custodial questioning will afford the government the broadest range of options to address the threat posed by the individual, including the option of an Article III prosecution.

These responses are current as of 7/3/12

c. Do you agree that in international terrorism cases time is of the essence but that it may take weeks or months to elicit intelligence from a captured combatant?

Response:

It can take significant time to elicit intelligence from a captured suspected terrorist, as it can to obtain information from an arrested criminal suspect. Nonetheless, in some cases we have had great success in quickly obtaining intelligence information from terrorist suspects in criminal investigations even when they have been advised of their *Miranda* rights.

12. Do you agree with the argument made by some that the United States is not part of the battlefield in the War on Terror? If so, why do you agree? If not, why not?

Response:

The FBI defers to those in a better position to respond to this inquiry. We note, though, that it is longstanding practice to use criminal law authorities to detain and interrogate terrorist suspects in the United States. This practice is beneficial because there is a substantial body of law interpreting these authorities, enabling us to anticipate whether evidence acquired through a particular technique is likely to be admissible in an Article III court. Because evidence that is admissible in an Article III court is admissible in a range of other contexts, such evidence would afford the government the broadest range of options to address the threat posed by the individual.

These responses are current as of 7/3/12

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

RICHARD J. DURBIN

 ILLINOIS

 ASSISTANT MAJORITY LEADER

SUBMISSIONS FOR THE RECORD

United States Senate
 Washington, DC 20510-1504

COMMITTEE ON APPROPRIATIONS

 COMMITTEE ON FOREIGN RELATIONS

 COMMITTEE ON THE JUDICIARY

 COMMITTEE ON RULES
 AND ADMINISTRATION

March 27, 2012

The Honorable Robert Mueller
 Director
 Federal Bureau of Investigation
 935 Pennsylvania Avenue, NW
 Washington, D.C. 20535

Dear Director Mueller:

I write to express my concern about the FBI's failure to adequately address inappropriate counterterrorism training that was provided to FBI agents.

Publicly released documents show that FBI agents received counterterrorism training based on crude stereotypes of American Muslims and Arab Americans. For example, agents were told that, "Islam is a highly violent radical religion," "mainstream American Muslims are likely to be terrorist sympathizers," and the "Arabic mind" is "swayed more by ideas than facts." These statements are inconsistent with American values of freedom and tolerance and the views of mainstream Democrats and Republicans. For example, former President George W. Bush often spoke about the true nature of Islam, saying on one instance, "All Americans must recognize that the face of terror is not the true faith – face of Islam. Islam is a faith that brings comfort to a billion people around the world. It's a faith that has made brothers and sisters of every race. It's a faith based upon love, not hate."

I raised this issue with Attorney General Eric Holder at a Senate Judiciary Committee hearing on November 8, 2011. Attorney General Holder testified that the FBI training in question is, "flat-out wrong and does not reflect the view of the Justice Department and the FBI." He explained that this training harms our counterterrorism efforts: "That kind of misinformation can really undermine the substantial outreach efforts that we have made and really have a negative impact on our ability to communicate effectively, as we have in the past, with this community." Similarly, John Brennan, President Obama's top counterterrorism advisor, characterized the training as "substandard and offensive," and said it "runs completely counter to our values, our commitment to strong partnerships with communities across the country, our specific approach to countering violent extremist recruitment and radicalization, and our broader counterterrorism efforts." In testimony to the Senate Judiciary Committee on December 14, 2011, you also criticized this training, testifying, "It does not represent the view of the FBI. ... I believe our relationship with the Muslim community is very good. Things like this set it back."

I appreciated your call last December to update me on the FBI's review of its training materials on Islam. I understand that the FBI has now completed its review of training materials and that FBI officials briefed Senate Judiciary Committee staff on the review's results last week. I commend you for ordering this review, which was clearly warranted based on the materials that

711 HART SENATE OFFICE BUILDING
 WASHINGTON, DC 20510-1504
 (202) 224-2152
 TTY (202) 224-6180

230 SOUTH DEARBORN, 38TH FLOOR
 CHICAGO, IL 60604
 (312) 353-4952

526 SOUTH EIGHTH STREET
 SPRINGFIELD, IL 62703
 (217) 492-4062

1504 THIRD AVENUE
 SUITE 227
 ROCK ISLAND, IL 61201
 (309) 788-9173

PAUL SIMON FEDERAL BUILDING
 210 W. CHERRY STREET
 SUITE 115-D
 CARBONDALE, IL 62901
 (618) 351-1122

durbin.senate.gov

have been made public. However, I am concerned about the FBI's plans for responding to the review's findings.

First, I was disturbed to learn about the content of the training materials that FBI investigators discovered during the review. I understand that investigators identified 876 pages and 392 presentations that included offensive materials. FBI briefers shared copies of a handful of these materials with Senate Judiciary Committee staff, although staff were required to return these copies to the FBI at the conclusion of the briefing. Among other statements included in these materials:

- One slide said, "Under certain circumstances, the FBI has the ability to bend or suspend the law and impinge on freedoms of others."
- Another slide, entitled "Establishing relationships," stated, "Never attempt to shake hands with an Asian" and "Never stare at an Asian" "Never try to speak to an Arab female prior to approaching Arab male first."
- Another slide, entitled "Control and Temper," stated that the "Western Mind" is "even keel" and "outbursts exceptional," while in the Arab World, "Outbursts and lose of control expected" and "What's wrong with frequent Jekyll and Hyde temper tantrums?"

Second, I am disappointed that the FBI apparently does not plan to produce a written report on its review. Moreover, the FBI does not plan to provide the inappropriate training materials identified in its review to Congress or the American people. FBI officials said that Judiciary Committee staff could review the training materials at FBI headquarters, but that the FBI would not provide these documents to the Committee. This is inconsistent with the FBI's responsibility to cooperate with Congressional oversight. FBI officials also told Judiciary Committee staff that the FBI does not plan to make public the training materials. I believe that sunlight is the best antiseptic, and that making public the results of the FBI's review would be an important step to restoring the trust of the American people, especially American Muslims and Arab Americans.

Third, I am concerned that no one has been held accountable for providing this training, which, according to the Attorney General of the United States, has undermined our counterterrorism efforts. The FBI has not publicly apologized to the American-Muslim and Arab-American communities and it is my understanding that no one has been disciplined. I understand that one of the individuals responsible for some of the training has been reassigned, but, according to FBI briefers, he was responsible for only "a small minority" of the offensive materials. It is unclear whether other responsible individuals continue to train FBI agents on Islam.

Next, it is unclear that the FBI has taken sufficient steps to undo the damage done by offensive training materials. It was my understanding from our conversation in December that the FBI's training review would identify FBI agents who received inappropriate training. However, FBI briefers told Senate Judiciary Committee staff last week that the review did not include training recipients. If the FBI does not identify agents who received inaccurate information and take steps to retrain them, there is a real risk that agents will be operating on false assumptions about Arab Americans and American Muslims. This could harm

counterterrorism efforts by leading FBI agents to target individuals based on their religion or ethnicity, rather than suspicion of wrongdoing.

Moreover, the review of training materials did not extend to FBI intelligence analyses of Islam and American Muslims. Unfortunately, the distorted view of Islam presented in FBI training seems to have affected some FBI analyses. For example, FBI Intelligence Assessment, which has been made public, claims that wearing traditional Muslim attire, growing facial hair, and frequent attendance at a mosque or prayer group, are all indicators of possible extremism. However these innocent behaviors, which are protected by the First Amendment freedom of religion, could simply indicate that an individual is a devout Muslim.

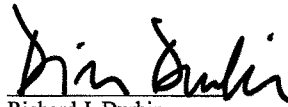
Finally, I fear that the FBI has not taken adequate measures to prevent problematic training in the future. A panel of experts has produced "FBI's Guiding Principles: Touchstone Document on Training," a 3-page document to provide guidance to trainers. However, this document, which was posted on the FBI's website last week, does not provide any specific direction on the content of training on Islam. It was my understanding from our December conversation that the FBI's expert panel would produce a curriculum, not simply high-level guidance.

I respectfully request that you take additional steps to address inappropriate FBI training on Islam, including:

- Provide the offending training materials to the Judiciary Committee and unclassified versions of the materials to the American people;
- At the very least, reassign the individuals responsible for providing inappropriate training;
- Retrain FBI agents who received inappropriate training;
- Conduct a review of FBI intelligence analyses of Islam, American Muslims, and Arab Americans; and
- Produce a detailed training curriculum on Islam which has been reviewed and approved by experts in the field.

I look forward to your prompt response. Thank you for your time and consideration, and thank you for your service to our country.

Sincerely,



Richard J. Durbin
U.S. Senator



U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535-0001

April 17, 2012

The Honorable Richard J. Durbin
United States Senate
Washington, DC 20510-1304

Dear Senator Durbin:

Thank you for your letter dated March 27, 2012, regarding the FBI's review of its counterterrorism training materials. The review identified mistakes in our training materials; we regret those mistakes, and we are working to correct them. The FBI is committed to ensuring that its counterterrorism training is accurate, appropriate, and consistent with the FBI's standards and Core Values.

The FBI's review and remedial actions to address inappropriate training materials were thorough and comprehensive. More than 30 Agents and professional staff carried out the review over a period of months. The review compiled training materials dating back 10 years, including some 160,000 pages and 1,000 minutes of recordings. For critical aspects of the review, we relied on a five-person team that included three individuals from outside the FBI (but who otherwise work for the government) and two from within the FBI. The team possessed advanced academic training and experience in Islamic Studies, religion, international relations, Arabic, and the history of the Middle East, and held degrees from major American and international universities. This combination of backgrounds in the study of religion and culture, as well as experience and training in counterterrorism and countering violent extremism, gave the team a collective expertise on the issues under review.

The review highlighted the need for mandatory processes to review and standardize all future training material, and we have taken significant steps towards achieving that goal. Only materials that are validated through such processes (or that were validated in the current review) will be used in future counterterrorism training.

Your letter cites three slides from the more than 160,000 pages reviewed and quotes select pieces of those slides. The FBI agrees that these slides were inappropriate. It is important to understand, however, that these slides do not reflect the overwhelming majority of training provided to our Agents and professional staff (indeed, 99.5% of the materials were deemed appropriate by the review team).

The Honorable Richard J. Durbin

News accounts have focused on one of those three slides and inaccurately claimed that the FBI taught Agents that they can "bend or suspend the law." I want to assure you that FBI personnel were not and are not taught that they can bend or suspend the law. The embedded "notes view" of the slide reflects that the instructor intended to explain that laws such as the Foreign Intelligence Surveillance Act permit the FBI to take actions ordinarily prohibited by law. Personnel who used this slide were interviewed and confirmed that this was the slide's intended meaning - though plainly the slide was poorly phrased. Of course, rigorous obedience to the Constitution is one of the FBI's Core Values and a fundamental underlying principle of all our training.

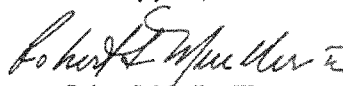
As to the other slides cited in your letter, we have taken steps to ensure that FBI personnel are not operating on false assumptions about Arab Americans and Arab Muslims. We have provided all field offices with a summary of the review's findings. We have also provided all field offices with examples of training slides that were inappropriate or inaccurate, along with a discussion of what was wrong with the material and why it was wrong. Finally, we are taking steps to ensure that all FBI personnel have accurate information about the basic tenets of Islam and Arab Americans and Arab Muslims.

Many of the 876 pages identified in the review have been released to the public in response to a request under the Freedom of Information Act (FOIA). We have also released to the public over 4,500 pages of basic training materials used at the FBI Academy in connection with the same FOIA request. A complete set of all the materials at issue is available to you and your staff for a full review. We have extended this invitation to Senate and House members and staff. To date, one member, as well as staff for other members, has reviewed the materials. I encourage you and your staff to do the same.

Finally, we interviewed personnel responsible for the materials to determine the purpose, context, specific use, and the intended audience for the material. Each was made aware that his/her training material was not acceptable for one or more reasons, and overall, was not consistent with FBI Core Values. Each was also made aware that he/she could no longer use the training materials at issue. We are continuing to look at the performance of certain individuals to determine what additional steps, if any, may be necessary.

I appreciate all that you do to help the FBI in its mission to protect the Nation. I look forward to working with you on this and other issues.

Sincerely yours,



Robert S. Mueller, III
Director



Counterterrorism Training Material Review

In 2011, training material came to the attention of FBIHQ that was inconsistent with FBI's highest professional standards and the organization's Core Values. Beginning in September 2011, the FBI conducted a comprehensive diagnostic review of FBI counterterrorism training material in an effort to determine whether additional similar material existed and, if so, to take appropriate action.

This report summarizes the results of the review. The report is divided into three sections. Section I describes the process to identify and review counterterrorism training materials developed and used over the last 10 years. Section II describes the findings: the quantity of materials revised or removed from use and a description of other steps taken. Finally, Section III describes plans to establish review processes to ensure that all training materials are reviewed and validated in the future.

I. The Review Process

A. Phase I -- Material Collection

Phase I of the review began in September 2011 by collecting counterterrorism training material¹ used since 2001 from FBI field offices, as well as the Counterterrorism, Training, International Operations, and Cyber Divisions, and the Directorate of Intelligence. This process also included a data call to all FBI components and a search of FBI record systems.

In total, the review collected 163,446 pages of training material (4,754 presentations) and 1,119 minutes of audio and video recordings.

B. Phase II -- Material Review

Phase II of the review began in October 2011 and consisted of a detailed review of all training material collected during Phase I. The primary review team consisted of 25 Assistant Inspectors in Place (AIIP) under the leadership of an Inspector. The AIIP team oversaw the collection, inventory, and initial review of the material in collaboration with a team of Subject Matter Experts (SMEs), who were selected with the assistance of the Combating Terrorism Center at West Point.

To facilitate an independent, objective, and academically rigorous review process, the FBI relied on the SME team for critical aspects of the review. The SME team consisted of five individuals, three of whom were from outside the FBI (but who held

¹ Training materials subject to this review included slides, talking points, note pages, handouts, audio/video files, and other related complementary materials developed, prepared, or acquired for use in delivering training. The review did not include any material(s) developed, prepared, or acquired for use by non-FBI personnel (i.e., individuals other than full-time, part-time, or contract personnel) who accepted an invitation by the FBI to provide training, except where such materials were contemplated for future availability in the FBI's Automated Case System, Sentinel, Virtual Academy, or intranet.



government affiliations) and two from within the FBI. The SME team possessed advanced training and experience in Islamic Studies, Religion, International Relations, Arabic, and History of the Middle East, and held degrees from major American and international universities. This combination of backgrounds in the study of religion and culture, and experience in training on counterterrorism and countering violent extremism, gave the group a collective expertise on the issues under review in the training material.

The SME team, in conjunction with an attorney from the FBI's Office of the General Counsel, Privacy and Civil Liberties Unit, prepared a document entitled *Guidelines for Training on Counterterrorism and Countering Violent Extremism* (hereinafter *Guidelines*), attached at Addendum 1, for the review process. The *Guidelines* emphasized the need to distinguish between lawful activities (including those that are constitutionally protected) and illegal action that may be taken in whole or in part based on extremist ideology. In addition to guiding the review, the *Guidelines* are intended to support the development of future training, as further described in Section III, and, therefore, may change over time, as appropriate. The SME team and OGC attorney also provided training to the AIIP team prior to the initiation of Phase II.

The AIIPs conducted an initial review of all training material using the *Guidelines*. Materials determined by the AIIPs to be inconsistent with the *Guidelines* were referred to the SME team for further review. Materials determined by the AIIPs to be consistent with the *Guidelines* -- and, therefore, not referred for SME review -- were re-distributed to other AIIPs for a secondary peer review. This two step process ensured that two independent people reviewed every document. In addition to this second review, the SME team reviewed a random sample of training material not referred for SME review during Phase II.

The SME team conducted an independent review of all materials determined by the AIIPs to be inconsistent with the *Guidelines*. The SME team made final decisions on the propriety of the material, and whether the material required removal or could be corrected and retained.

II. The Review Findings

A. Materials Removed or Edited

The final SME team review determined that 876 pages of training materials were inconsistent with the *Guidelines*. The 876 pages were contained within a total of 392 presentations. These presentations were either removed from use or edited per guidance from the SME team.

After the SME review was completed, a separate smaller team of Inspectors-In-Place grouped the 876 pages into four categories as follows (examples of material edited or removed is contained in Attachment 2):



Pages Reviewed and Categorized		
Total Reviewed	163,446	
Category	Pages By Category	% By Category
Factual Error ²	82	0.05%
Poor Taste ³	84	0.05%
Stereotype (Non Correctable) ⁴	269	0.16%
Lacks Precision ⁵	441	0.27%
TOTAL CATEGORIZED	876	0.54%

B. Interviews

Following the document review, the AIIPs interviewed the authors and/or presenters of documents identified for editing or removal from use. The purpose of the interviews was to determine the underlying source of materials and the context in which the materials were presented. The interviewers also explained to the authors/presenters why the materials were not consistent with the FBI's standards and Core Values and why, going forward, they would not comply with the *Guidelines*.

III. Plan for the Future

Going forward, the Training Division, the HQ Operational Divisions, and the Special Agents In Charge Advisory Committee (SACAC) are developing corporate policy to ensure that all FBI training adheres to the FBI's Core Values and satisfies the *Guidelines*. The Training Division and all operational divisions will review and standardize all training conducted at the FBI Academy as part of FBI core skills and career path training. All field office training, including training to law enforcement partners, will also be subject to a field office review process governed by the SAC. No training produced or presented by the FBI will be exempt from this review process.

² Factual Errors refers to documents that contain factually incorrect statements, however, the factual errors do not adversely impact the FBI's ability to meet training objective(s).

³ Poor Taste refers to documents with content which could be viewed as having inappropriate humor or that makes offensive comparisons regarding a specific religious or ethnic group.

⁴ Stereotype refers to documents that contain prejudicial or stereotypical comments about a particular religious or ethnic group so as to make the documents non correctable.

⁵ Lacks Precision refers to documents that need to be refined or edited to make clearer the learning objective(s). These documents are deemed to be correctable and can be used in training after appropriate SME edits.



Conclusion

The counterterrorism training material review determined that the vast majority of the FBI's counterterrorism training is accurate, appropriate, and consistent with the FBI's standards and Core Values. However, the review also identified a small segment of training material that was factually inaccurate, in poor taste, based on an inappropriate stereotype or lacking appropriate precision. The review's findings highlighted the fact that the FBI lacks a centralized process to ensure that all training material is reviewed, validated, and consistent with our Core Values and the Guidelines.

Training which does not adhere to standards or our Core Values does not serve the FBI's investigative priorities. Providing training which is offensive or politically motivated does not serve the FBI in preparing personnel to work within our communities. We require a workforce that has a basic understanding of Islam, its history, and an understanding of Middle Eastern cultures so that we can successfully interact within our communities. Training must be objective and based in sound academia. The efforts described here contribute to that goal.

