AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–173

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MARCH 30, 2011

Serial No. J–112–12

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
71–557 PDF WASHINGTON : 2012

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

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut

CHUCK GRASSLEY, Iowa
ORRIN G. HATCH, Utah
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

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	81

WITNESS

Mueller, Robert S., III, Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC	5

QUESTIONS AND ANSWERS

Responses of Robert S. Mueller, III to questions submitted by Senators Klobuchar, Franken, Grassley, Hatch, Kyl and Sessions	34

SUBMISSIONS FOR THE RECORD

Mueller, Robert S., III, Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC, statement	83

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

WEDNESDAY, MARCH 30, 2011

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

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Kohl, Schumer, Durbin, Klobuchar, Franken, Coons, Blumenthal, Grassley, Sessions, Kyl, and Graham.

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

Chairman LEAHY. Today the Judiciary Committee will hear from Director Robert Mueller.

This fall, the Director will complete his 10-year term overseeing the FBI. He and I were talking out back earlier, and I do not know when I have seen 10 years go by so quickly, and I am sure the Director feels the same way. He took over just days before the attacks of September 11th. And I told him a reference from Elizabethan England, which I will not repeat here, in the hearing room at that time, but it did seem like everything—it was almost as though they were trying to give the Director his full 10-year term in about the first 10 days, with all that went on. He has overseen a major transformation of the Bureau. While the FBI continues to perform all the functions of a Federal law enforcement agency, it has greatly increased its role in ensuring our National security. There have been growing pains and false starts, but Director Mueller has managed this transformation of a large and well-established agency with great professionalism and focus, and he will leave at the end of his tenure a better Bureau than he had when he came in.

The Director has aggressively pursued both law enforcement and national security objectives while maintaining a strong commitment to the values and freedoms we hold most dear as Americans. In commemorating the 100th anniversary of the FBI several years ago—and I remember sitting there listening to the Director as he said this—he said:

"It is not enough to stop the terrorist—we must stop him while maintaining his civil liberties. It is not enough to catch the criminal—we must catch him while respecting his civil rights. It is not enough to prevent foreign countries from stealing our secrets—we must prevent that from happening while still upholding the rule of law. The rule of law, civil liberties, and civil rights—these are not

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

our burdens. They are what make us better. And they are what have made us better for the past 100 years."

I was in that audience when he said that. I think it is fair to say the audience went across the political spectrum, and his statement was greeted with long and sustained applause.

I have tried to advance these same objectives with carefully calibrated criminal justice legislation like the Justice For All Act and national security legislation like the USA PATRIOT Act reauthorization proposal that recently passed through this Committee. But I am gratified that the Director shares my commitment to working to keep all Americans safe while preserving the values of all Americans.

I appreciate that the FBI has shown signs recently of real progress on issues vital to this Committee and to the country. National security and counterterrorism are central to the FBI's mission. But it has been heartening to see this steady stream of important arrests of those who would do this country harm.

Earlier this month, the FBI arrested Kevin Harpham for planning to bomb a march in honor of Martin Luther King Day in Spokane, Washington. Mr. Harpham reportedly had ties to white supremacist groups, and the plot he is accused of planning came dangerously close to succeeding. Had it succeeded with the bomb that he had, the results could have been devastating to a large crowd of people, and I commend the FBI for making this arrest, which shows the continuing threat posed by domestic terrorism and makes very clear that no one ethnic group has a monopoly on terror.

Now, in the last Congress, we made great strides toward more effective fraud prevention and enforcement. I worked hard with Senator Grassley and others to craft and pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade. It adds resources and statutory tools for effective prevention, detection, and enforcement of mortgage fraud and financial fraud. We have worked hard to ensure that both the health care reform legislation and Wall Street reform legislation passed last year had important new tools for cracking down on fraud. Senator Grassley and I are hard at work now on new legislation to provide greater support for aggressive enforcement of our fraud laws.

I am pleased to see that the FBI has been taking advantage of this heightened support for fraud enforcement. They have greatly increased the number of agents investigating fraud. They have led to more fraud arrests, but also—and the taxpayers should be happy about this—they have led to greater fraud recoveries. And I am glad that the FBI has maintained its historic focus on combating corruption. I would hope that they would continue to crack down on the kinds of fraud that contributed so greatly to our current financial crisis and on corruption that undermines Americans' faith in their democracy.

Last, I have been heartened to see that the FBI's statistics continue to show reductions in violent crime nationwide despite the painful recession, and I commend the FBI for their work in combating violent crime. I hope that Congress will continue to provide the urgently needed assistance to State and local law enforcement,

which has been vital to keeping crime down throughout the country.

Then, of course, areas of major concern include the FBI's continuing struggles with modernizing its technology and information-sharing systems. We will have vigorous oversight, and I know that today's hearing will shed light on these areas.

I thank Director Mueller for returning to the Committee, for his responsiveness to our oversight efforts, but especially for his personal example and impressive leadership over the past decade in returning the FBI to its best traditions. If you get to know the Director and his family, you can see he carries the same values to work, and I commend him for that.

I also would say I commend him for the times when difficult things were happening, he has called me at home or on the road or in Vermont, and he actually traveled to Vermont with me to talk about it. That meant a great deal and means a great deal. And, of course, I thank the hard-working men and women of the FBI. And, again, without going into our personal conversations, earlier the Director and I were talking about how fortunate we are to have the kind of men and women who have put their lives on hold to uphold what is needed in our country.

Senator Grassley.

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

Senator GRASSLEY. Thank you. Mr. Chairman, oversight of the FBI is probably one of the most important oversight hearings that you have, and so I thank you.

I would take a moment to publicly thank you, Director Mueller, for your service to America, and I do that just in case this might be the last time as Director of the FBI you are before this Committee. But I will bet you after you are in private life you will be asked to testify on various things before Congress in that capacity because of your experience.

While we have had our share of disagreements, Director Mueller, I have always appreciated your candor and your willingness to work with us to get answers even if we do not always agree with what those answers are. For instance, I know there is a lot of agreement between you and me on the need to extend the PATRIOT Act provisions that are set to expire in May. The three expiring provisions of the PATRIOT Act are very important tools used by law enforcement and the intelligence community to protect us from threats to our National security. They are vital to our ability to investigate, identify, track, and deter terrorists.

It was recently revealed that the FBI successfully utilized a Section 215 order as part of the investigation that prevented a terrorist attack planned by a Saudi national in Texas. In that case it was revealed that the individual in question purchased bomb-making materials such as 3 gallons of sulfuric acid, clocks, chemistry sets, and a gas mask from online retailers Amazon.com and eBay. This case is the latest of many examples of successes of the PATRIOT Act provisions and your successful use of that.

Given the numerous threats we face and the fact that the three expiring provisions have not been found to have been abused, the

Senate should work to reauthorize the expiring authority without amendment.

Aside from the critical national security authority we need to reauthorize, I want to today eventually ask Director Mueller about a recent report that was issued by the Homeland Security and Governmental Affairs Committee released in February entitled, "A Ticking Bomb" that examined the tragic shootings at Fort Hood that occurred November 2009. That report highlighted a number of problems at both the Department of Defense and the FBI and found "systematic failures in the Government's handling of the Hasan case."

I was troubled to hear allegations contained in the report, including that an analyst on a Joint Terrorism Task Force was not provided full access to a key FBI data base simply because he was from a non-FBI agency. I want to hear from the Director whether he agreed with some of these key findings, what is being done to correct any deficiencies in the way terrorism cases are reviewed, and whether information sharing has been improved.

I will also ask the Director some questions about FBI employee personnel matters. I have long been concerned about the plight of whistleblowers within the FBI. Director Mueller has made it a priority to instruct all employees of the FBI that retaliation against whistleblowers will not be tolerated, but, unfortunately, that directive has not always been followed by agents in the field, and I find one case particularly troubling.

In 2007, the Department of Justice Inspector General issued a memorandum finding that a 30-year non-agent employee of the FBI, Robert Kobus, was retaliated against for protected whistleblowing. The Inspector General found that, "The FBI management in the New York Field Division improperly moved Kobus from the position of a senior administrative support manager to several nonsupervisory positions." One of those positions included being demoted to OSHA safety officer. The retaliation was blatant and included moving his office to a cubicle on a vacant 24th floor of the FBI building. The Inspector General ultimately concluded that the decision to move him was in retaliation for disclosing wrongdoing to a special agent in charge of the field office, in this case an attendance fraud by FBI agents. This is exactly the type of retaliation against whistleblowers that should never occur.

So I am working on a request that I shared with Chairman Leahy—you may not know about it, but I have given it to your staff—hoping that we can work together on this issue. But I would also request that the Government Accountability Office conduct a top-to-bottom review of the Department of Justice's process for dealing with FBI whistleblowers. Delays like the one in the Kobus case send a clear signal to potential whistleblowers that reporting wrongdoing will only end up in an expensive bureaucratic mess.

Another area of concern that I have relates to the FBI employee misconduct. In January of this year, the internal FBI Office of Professional Responsibility documents were leaked to the press. Those documents contained a number of shocking allegations about misconduct committed by employees of the FBI. An example: The document detailed FBI agents who were dismissed because they were arrested for drunk driving, engaged in improper relationships with

FBI informants, leaked classified information to reporters, sought reimbursement for expenditures they never made, and in one instance brought foreign nationals back into the FBI's space after hours. I want to know more about these penalties, how they were determined. I think it is necessary and important to know in light of the fact that the Inspector General found in the May 2009 report that there is a perception among FBI employees that there is a double standard for discipline among higher-ranking and lower-ranking employees.

Director Mueller, over the past 8 months, I have been investigating systemic problems at the Philadelphia Public Housing Authority—outlandish salaries, sexual harassment settlements, and excessive legal billings, just to name a few of the problems, and I want to express my appreciation regarding the FBI's ongoing investigation and recent seizure of expensive luggage purchased as gifts by the Philadelphia Public Housing Authority, and I hope the FBI follows through vigorously on any criminal violations that may have occurred at the Philadelphia Public Housing Authority.

Finally, I want to ask the Director about the fiscal year 2012 budget request that was submitted to Congress. I continue to have concerns with the FBI's agency-wide case management system known as Sentinel. I want to know when this is going to end, how much more taxpayers' money will be necessary, and how the FBI plans to maintain the older case management data base as part of the new system. After a decade of upgrading the system, not another dime of taxpayers' money should be awarded until the FBI can prove the system will work and will be done on time.

That is a lot to cover. I thank you for your patience as I cover those items.

Chairman LEAHY. Thank you very much.

Director Mueller, please go ahead, sir.

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

Mr. MUELLER. Thank you and good morning, Chairman Leahy and Ranking Member Grassley and other members of the Committee who are here today. I appreciate the opportunity to appear before the Committee.

I will start by saying that the FBI faces today unprecedented and increasingly complex challenges. We must identify and stop terrorists before they launch attacks against our citizens. We must protect our Government, businesses, and critical infrastructure from espionage and from the potentially devastating impact of cyber-based attacks. We must root out public corruption, fight white-collar and organized crime, stop child predators, and protect civil rights.

We must also ensure we are building a structure that will carry the FBI into the future by continuing to enhance our intelligence capabilities, improve our business practices and training, and develop the next generation of Bureau leaders. And we must do all of this while respecting the authority given to us under the Constitution, upholding civil liberties, and the rule of law.

The challenges of carrying out this mission have never been greater as the FBI has never faced a more complex threat environment than it does today. Over the past year, the FBI has faced an extraordinary range of threats from terrorism, espionage, cyber attacks, and traditional crime. A few examples.

Last October, there were the attempted bombings on air cargo flights bound for the United States from Yemen, directed by al Qaeda in the Arabian Peninsula. Last May, there was the attempted car bombing in Times Square, aided by TTP in Pakistan. These attempted attacks demonstrate how al Qaeda and its affiliates still have the intent to strike inside the United States.

In addition, there were a number of serious terror plots by lone offenders here in the United States. Their targets ranged from the Martin Luther King Day march in Spokane, Washington, as mentioned by the Chairman, to a Christmas tree lighting ceremony in Portland, Oregon; to subway stations in the Washington, D.C., Metro system. And while the motives and methods for these plots were varied, they were among the most difficult threats to combat.

The espionage threat persisted as well. Last summer, there were the arrests of ten Russian spies, known as "illegals," who secretly blended into American society in order to clandestinely gather information for Russia. And we continued to make significant arrests for economic espionage as foreign interests seek to steal controlled technologies.

The cyber intrusion at Google last year highlighted the potential danger from a sophisticated Internet attack. And along with countless other cyber incidents, these attacks threaten to undermine the integrity of the Internet and to victimize the businesses and persons who rely on it.

In our criminal investigations, we continue to uncover billion-dollar corporate and mortgage frauds that weaken the financial system and victimize investors, homeowners, and ultimately taxpayers. We also exposed health care scams involving false billings and fake treatments that endangered patients and fleeced Government health care programs.

The extreme violence across our southwest border continued to impact the United States. As we saw the murders last March of American consulate workers in Juarez, Mexico, and the shooting last month of two U.S. Immigration and Customs Enforcement agents in Mexico. And throughout the year, there were numerous corruption cases that undermined the public trust and countless violent gang cases that continued to take innocent lives and endanger our communities.

As these examples demonstrate, the FBI's mission to protect the American people has never been broader, and the demands on the FBI have never been greater. And to carry out these responsibilities, we do need Congress' continued support more than ever.

Let me briefly discuss two areas where Congress can help the FBI with its mission. First, we do encourage Congress to reauthorize the three FISA tools that are due to expire later this spring; the roving intercept authority is necessary for our national security mission and provides us with tools similar to what we use in criminal cases already and have used for a number of years.

The business records authority permits us to obtain key documents and data in our national security cases, including in our most serious terrorism matters. And the lone-wolf provision is important to combat the growing threat from lone offenders and homegrown radicalization. These authorities, all of which are conducted with full court review and approval, are critical to our national security.

Second, the FBI and other Government agencies are now facing a growing gap in our ability to execute court-approved intercepts of certain modern communications technologies. We call this the problem of going dark. With the acceleration of new Internet-based technologies, we are increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking, as well as to terrorism and espionage.

Let me emphasize at the outset that collecting this evidence has been approved by a court, but because the laws have not kept pace with the changes in technology, often we cannot obtain the information responsive to the court orders from the communications carrier. And we look forward to working with this Committee and Congress on the legislative fixes that may be necessary to close this gap and preserve our ability to protect all Americans.

Last, let me say a few words about the impact of the continuing budget resolutions on the FBI and on our workforce.

The support from this Committee and Congress has been an important part of transforming the FBI into the national security agency it is today. But for our transformation to be complete, we must continue to hire, train, and develop our cadre of agents, analysts, and staff to meet the complex threats we face now and in the future.

Under the current levels in the continuing resolution, the FBI will have to absorb over $200 million in cuts, and without any change, the current CR will leave us with over 1,100 vacant positions by the end of the year. Put simply, these cuts would undermine our efforts to continue to transform the Bureau and undermine our efforts to carry out our mission.

I appreciate the opportunity to review the FBI's work in responding to the far-reaching threats we face today before you today. I also want to thank the Committee for your continued support, the support over the years that I have held this position, and not only support for me but most particularly for your support of the men and women of the FBI who do the work of this great institution.

Thank you and I would be happy to answer any questions, Mr. Chairman.

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

Chairman LEAHY. Well, thank you, Director, and again, I reiterate my personal feelings and appreciation for what you have done and for the openness you have shown when I have had questions, and others on the Committee. All Senators I think have found you to be very accessible.

Earlier this month—and I mentioned this in my opening statement about the FBI arresting Kevin Harpham in connection with a plot to bomb a parade in honor of Martin Luther King Day in

Spokane, Washington. And what I have read in the press is that the bomb was very sophisticated. The plot almost succeeded. With the large number of people around there, at looking at some of the press photographs, if the bomb had gone off, the results would have been horrible.

Now, he reportedly had ties to white supremacist groups, and I mention this only because I do not want us to lose sight of the fact that domestic terrorism may not be as visible as international terrorism, but also the threat to us just as Timothy McVeigh in Oklahoma City and others.

What is the threat posed by domestic terrorism? How would you just generally—not this particular case, but generally, how do you see the threat of domestic terrorism?

Mr. MUELLER. Well, we have not lost sight, even with September 11th, of the devastation that was wreaked by McVeigh in Oklahoma City in 1995, and we have, certainly before then but most particularly since then, had domestic terrorism almost as important an issue as the international terrorism that we have seen over the years. Whether it be white supremacists, militia extremists, sovereign citizen extremists, we continue to undertake investigations with adequate—where we have the predication to make certain that these groups do not present terrorist threats.

I will tell you that most concerning is, yes, the groups themselves in some ways, but most concerning are the lone wolves, those persons who may have had some loose affiliation with one of these groups but may have been rejected by the group as being too extreme or individually found the group was not extreme enough and then on their own undertake an attack. And so I would say the possibility of activity from a lone wolf is the thing that we are most concerned about——

Chairman LEAHY. Those are the people that would be the hardest to track, I would take it.

Mr. MUELLER. That is correct. They do not communicate with any others. It is really difficult to put into place the capabilities of alerting us when one of those individuals looks like they want to go operational.

Chairman LEAHY. The Unabomber, people like that.

Mr. MUELLER. Exactly.

Chairman LEAHY. It is very hard. I agree with you, and I raise this just because I would hate to have everybody lose sight of the fact in a Nation of 300 million people and the size of our country that we do face questions of domestic terrorism, and we have to, not just at the FBI level but State and local and others, keep track of that, too.

Last week, the press released an FBI memorandum providing guidance to the field on the interrogation of terrorist suspects arrested in the United States. Now, you could have people playing on all sides of the debate about how to treat terrorism suspects. As far as I could tell, the memo essentially reiterates current law. When I first became a prosecutor, *Miranda* came down. You had *Escobido* and then *Miranda*. I remember working with the police within my jurisdiction as to how you adapt to it. You have in your regular training programs for any new FBI agent how to do it. This memo reiterates the requirements of the *Miranda* decision, and it restates

the narrow parameters of the public safety exception, and there has always been—contrary to some of the plain rhetoric, there has always been a public safety exception, and it makes no changes to the requirements governing presentment of a suspect in court. If the agents believe the suspect has valuable intelligence, they can continue the interrogation even beyond the recognized parameters of the public safety exception and understanding the possible exclusion in court.

I think you were wise to do it this way and not do it through trying to make a congressional change, and I will get into that in a moment. But have these procedures been effective in the past? You have had this in place now for a while. Have they been effective? Do you think they will be effective in the future?

Mr. MUELLER. I do think they have been effective and will continue to be effective in the future. We are in some sense in uncharted but guided territory in the sense that the *Quarles* decision issued by the Supreme Court that establishes the public safety exception was applicable to a discrete set of facts relating to a robbery, and what we have to anticipate is how that public safety exception translates to the area of terrorism. And our guidance errs on the side of obtaining that information we need to prevent the next terrorist attack, but within what we think would be the parameters of the public safety exception if and when the Supreme Court has an opportunity to look at how expansive that particular exception is.

Chairman LEAHY. And you have to assume they will. I recall being in a long meeting with the President, and I believe Attorney General Holder joined the meeting partway through. We were talking about whether we would make changes—try to make changes legislatively to *Miranda*. I argued that you cannot really do that. The *Dickerson* case, the Supreme Court said that *Miranda* is a constitutional decision, and a legislative act could not overrule that. But as a constitutional decision, it has been your experience, I take it, that the Supreme Court has carved out certain areas that show practicality in there, for want of a better word.

Mr. MUELLER. Well, I think we have to wait and see what the Supreme Court does. In the meantime, our principal responsibility when it comes to counterterrorism is stopping the next terrorist attack, and consequently, you look at each case as an opportunity to gather that intelligence and information that will stop the next terrorist attack. And that is foremost on our minds, but doing that within the construct that has been given to us by the Congress and the Supreme Court.

Chairman LEAHY. And this memorandum gives some flexibility in——

Mr. MUELLER. It does.

Chairman LEAHY. Thank you. I mentioned your tenure began just before the September 11th attacks and will wrap up just before the tenth anniversary of that. We have seen a big transformation. Now, your successor, whoever he or she may be, is going to sit down with you, if they are at all wise—certainly I would recommend it—to talk about what has happened in the last 10 years and certainly the views of the next 10 years. When you hand that leadership over, what would you say is the most—what would you

tell them is the most effective way to manage the extraordinary amount of data that is gathered by the FBI? It is like a tsunami, the data that comes in there. How do you do that and identify threats and hold our values? What kind of advice would you give? That will be my last question.

Mr. MUELLER. Well, generally, my advice would be to rely on the people in the FBI. I started a week before September 11th. I was new. I did not know really how the FBI operated other than looking at it from afar as an Assistant United States Attorney, and the remarkable thing is how that organization pulled together to undertake the responsibilities of responding to September 11th. And so regardless of what one does as the Director, it is the FBI as an organization and an institution that has the strength to carry us.

With regard to the tsunami of information that you talk about, one of the lessons we have learned since September 11th is there has been a profusion of databases, different databases given different authorities, and what we have needed over a period of time, and not only us but others in the intelligence community, are the capabilities for federated searches that enable you to pull out the pieces of information from disparate databases and put them together to prevent the next terrorist attack.

But as much as you can do this digitally, as much as you can do this with databases, it always is the human element, the personal element that ultimately is successful. And developing the persons who are capable of sifting through this data with the help of algorithms and the like is as important as developing the digital capability to sort through it. And so continuing to build the analytical cadre, continuing to build the type of agents and analysts and professional staff that no one understands, the technological area, but no one understands the human element of it is as important as anything else, and that is what we have tried to do, build up that capability since September 11th, and I would expect that my successor would continue on that path.

Chairman LEAHY. Thank you very, very much.

Senator Grassley.

Senator GRASSLEY. Director Mueller, I am going to start out with a question or two that probably you touched on in your testimony, but I think it is important that we get answers to specific questions. It is in regard to the PATRIOT Act. And you know the three provisions that are expiring. Do you agree that these three provisions should be made permanent?

Mr. MUELLER. Yes, sir.

Senator GRASSLEY. Have these three tools been useful to the FBI to prevent terrorist attacks on our country?

Mr. MUELLER. They have. Let me, if I can, briefly mention the business records provision has been used over 380 times. You alluded to an instance where it was used recently. It is absolutely essential that we have the ability to gather these records through that provision. Whether it be for identifying intelligence officers from other countries, these records enable us to get hotel records, travel records and the like, and without that capability, it would be difficult to develop the cases and the investigations in that arena as well as the counterterrorism arena without this provision.

The roving wiretap provision has been used more than 190 times. It is limited in the sense that we have to show that the individual for whom we wish this authority is trying to avoid surveillance, and, again, it is reviewed by the court before it is issued. And as I did mention in my testimony, we have had this capability on the criminal side of the house for any number of years. It has been very helpful in national security and important.

The one we have not yet used is the lone-wolf provision, but I still believe that that is important. We have come close to using it in several of our cases. The one thing I would point out there is that the only time it is to be used is on a non-U.S. citizen and with court approval. And, consequently, while we have not used that provision, with the profusion of lone-wolf cases domestically and, indeed, some internationally, my expectation is we will be using this in the future, and I believe that it is important that it be reauthorized.

Senator GRASSLEY. I think that your answer shows that if these provisions were not reauthorized or if they were substantially weakened by including new requirements, it would be detrimental to the agents in the field. Would that be a correct assumption?

Mr. MUELLER. Yes, sir.

Senator GRASSLEY. And kind of from your point of view whether any of these three provisions have been subject to any negative reports of finding abuse.

Mr. MUELLER. I am not aware of any.

Senator GRASSLEY. OK. Let me go to three other tools which are not set to expire and are not part of the needed reauthorization. These are the Foreign Intelligence Surveillance Act pen register and trap-and-trace orders, national security letters, and delayed notice search warrants. The FBI regularly uses pen register/trap-and-trace authority in both national security and criminal areas. Is that a correct assumption on my part?

Mr. MUELLER. Yes, sir.

Senator GRASSLEY. Under current law these authorities have the same legal standard, relevance. That is correct, isn't it?

Mr. MUELLER. Yes, sir.

Senator GRASSLEY. Do you believe increasing the legal burden on these investigative tools is necessary?

Mr. MUELLER. Speaking generally, I would say no, I believe we are at a point in time where there has been the appropriate balance between, on the one hand, the necessity for addressing the terrorist threat and threat from other criminal elements in the United States, and yet on the other hand, the protection of privacy, civil liberties. And I think that balance has been worked out satisfactorily over the years since September 11th.

Senator GRASSLEY. National security letters are an essential part of building blocks of national security investigations. They have never had a sunset in law. Do you think that they need one now?

Mr. MUELLER. I do not.

Senator GRASSLEY. Delayed notice search warrants are primarily a criminal tool, not a national security tool. Is that right?

Mr. MUELLER. That is correct.

Senator GRASSLEY. Has there been any criticism of their use that you know of requiring us to change the delay from 30 days to 7 days?

Mr. MUELLER. Not that I am aware of.

Senator GRASSLEY. Is there any advantage to decreasing the delay period?

Mr. MUELLER. Did you say decreasing the delay period?

Senator GRASSLEY. Yes.

Mr. MUELLER. I think the suggestion was decreasing it from——

Senator GRASSLEY. 30 to 7.

Mr. MUELLER. That is something we would have to look at the impact there, but I am not aware of any abuse or any activity that directs or mandates such a change. Let me put it that way.

Senator GRASSLEY. At least as of now then, I can conclude that you would not be able to say that you support a change at this point.

Mr. MUELLER. I would have to look at the legislation and, quite obviously, the last word is the Justice Department terms and views letter.

Senator GRASSLEY. Okay. I would like to go to the Electronic Communications Protection Act. There is a coalition called the Digital Due Process Coalition, business and interest groups supporting a probable cause standard for obtaining all electronic communications regardless of its age, the location, or storage facilities or the providers of access to information. Do you support raising the legal standard for obtaining electronic communications to a probable cause determination?

Mr. MUELLER. I do not, and that would be tremendously problematic in our capability of undertaking and successfully undertaking investigations to prevent terrorist attacks. We use the information, not the content of communications but the existence, in fact, of communications to make the case for probable cause that would enable us to utilize the more intrusive investigative powers that have been given to us by Congress. If that standard was to change, it would severely inhibit our ability to make those probable cause showings to the court in order to continue the investigation as is warranted.

Senator GRASSLEY. Let me ask you specifically along that line if you think the legal standard to obtain information through a pen register or trap-and-trace order should be increased to a probable cause or 2703(d) standard.

Mr. MUELLER. No, for the same reasons that I stated before.

Senator GRASSLEY. OK. Do you agree that a change like this would be unworkable and burdensome? I think you have answered that, that it would be burdensome.

Mr. MUELLER. I would have to look at the particular provision and look more closely at it to be able to answer that particular question.

Senator GRASSLEY. I have more questions, but I think my time is up. I am going to leave for a few minutes and go to Agriculture, but I will come back.

Chairman LEAHY. Thank you. Thank you very much.

I yield to Senator Kohl.

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

Director Mueller, I remember 10 years ago—it was like yesterday—when you came on board, and as with all of us, time goes by very, very quickly. But I want to express my deep, deep admiration and respect for you as a person and as an individual with the capabilities that you have and have demonstrated over the past 10 years. You have been a crucial asset to our country, and I along with, I think, everybody who has been connected with you over these past 10 years looks at your tenure in terms of how much it has done for our country and how much we owe you by way of appreciation.

Mr. MUELLER. Thank you, Senator.

Senator KOHL. I want to speak just a bit about what happened at Fort Hood. As you know, the Senate Homeland Security Committee released a report critical of the FBI. They said that the FBI conducted only a cursory investigation into evidence that existed that the shooter was frequently involved in talking with an al Qaeda-affiliated terrorist overseas. The report also said that the FBI failed to give the Pentagon full access to an FBI data base that likely would have sparked an in-depth inquiry that would most likely have avoided what occurred at Fort Hood.

Going forward, which is really all we need to be concerned about at this time, what can you tell us about new procedures that are in place that will head off another Fort Hood in the future?

Mr. MUELLER. I will say at the outset that this is one of—the pieces of information on the individuals responsible for Fort Hood were found in one of the thousands of cases we handle day in and day out. But what we found as a result of Hasan's incident, his attack on that day, is there were gaps that we had to fill.

Immediately afterwards, we looked at our procedures. We found that we could do a much better job at information sharing with DOD and, consequently, today elements of the Department of Defense serve on our National Joint Terrorism Task Force. They are in many of our Joint Terrorism Task Forces around the country, but most particularly we have a formalized process where we sit down and go through all the cases, whether a DOD case or our cases that may touch on DOD, so that we have before both entities a full review of those cases that may impact DOD.

Second, we have put into place technological improvements relating to the capabilities of a data base to pull together past e-mails and future ones as they come in so that it does not require an individualized search. So putting together a technological improvement to enhance our capabilities.

Last, we—not last, actually. Two more things. Third, what we had done is assure that we have not just one office that is reviewing, say, communications traffic but have a redundancy of review at headquarters as well to make certain that we do not miss something.

And, last, you alluded to an analyst's inability to either access or knowledge of a particular data base, and we underwent an extensive training initiative for all persons serving on Joint Terrorism Task Forces in the wake of what happened at Fort Hood to assure that not only the persons have access to the databases, but were knowledgeable and knew when and where to utilize those particular databases.

So I do believe that we have addressed the issues that came to our attention immediately after the Fort Hood incident.

Senator KOHL. Director Mueller, the ability of American companies to out-innovate and out-compete the rest of the world is more important today than ever. In 1996, I worked to pass the Economic Espionage Act. This is a law that makes it a Federal crime to steal trade secrets. And yet the FBI estimates that U.S. companies continue to lose billions of dollars each year when criminals do steal their trade secrets.

I am currently reviewing the Economic Espionage Act to see what improvements are needed to better protect American companies. As a first step in this process, I am introducing legislation to increase maximum sentences for economic espionage from 15 to 20 years and the Sentencing Guideline range.

Do you support these penalty increases? Will you work with me as we consider additional updates to the law? And do you have any suggestions as to what we should be doing?

Mr. MUELLER. I would have to, quite obviously, consult with Justice in terms of the response, but it seems to me that I would think we would look quite favorably on the suggestions of enhanced penalties in this arena. And, of course, we would work with you and your staff in terms of looking at what other areas might be improved through legislation.

Senator KOHL. Maybe you can respond to this. In 1996, we considered including a Federal civil private right of action as a tool for companies to combat and deter theft of trade secrets. At the time we decided to forgo this and rely on State trade secret laws. Other criminal laws like the Computer Fraud and Abuse Act contain companion Federal civil remedies for victims.

What are your views as to how prosecutions and investigations could be improved if a private right of action was available? Might you support a change of this sort?

Mr. MUELLER. I think we—and by "we," I mean ourselves and the Justice Department—would have to look and see what is in the statute. I might be leery at the outset of including a private right of action, maybe because I would be somewhat concerned about overlap and conflicts in terms of investigations, and it is something that I would think that we would have to look at very closely to determine what adverse impact there might be on our ability as the Government actor to pursue these cases if there was a private right of action. I am not saying there should not be. I am just saying that is something that we ought to look at closely before the Justice Department gives a position on whatever legislation that is proposed.

Senator KOHL. Finally, what advice would you give your successor in avoiding pitfalls that you experienced during your tenure?

Mr. MUELLER. Whew. I would say rely on the great people in the FBI, just a remarkable organization, remarkable grouping of people.

I think I would also say, when I have gotten in trouble, it is because I have not asked the hard questions and I have been satisfied with answers that were fine on the surface, but there were areas that I should have delved deeper and found out the answers myself. I could kick myself in some of those arenas.

One of the other things I would say is that it is important for us in the organization to understand what is necessary to protect the American public to grow and adjust to the new threats that are coming so much faster than they did 10, 15, or 20 years ago and be flexible and agile to address those threats, and the organization has to do what it needs to do for the American public as opposed to what we may enjoy or like doing as prosecutors or as agents. And the Bureau has always done that, and it is history, and we are going to have to do it, and do it swifter and faster in the future.

Senator KOHL. Thank you very much.

Senator Graham.

Senator GRAHAM. Thank you, sir.

I would like to acknowledge your service for probably one of the most challenging times in American history. I really appreciate what you have tried to do for our country in your whole force.

Mr. MUELLER. Thank you, sir.

Senator GRAHAM. You mentioned, I think, in your testimony about Border Patrol agents being killed. What is your assessment of the violence in Mexico? Are the border areas more dangerous? And where do you see this going in Mexico?

Mr. MUELLER. I think anybody looking at what has happened in the last several years along the border but also inside Mexico in terms of the increasing homicides, the breakdown of, to the extent that there was any cartel—I do not want to say "justice," but restraint—has long since been lost with the increase in homicides despite the efforts and intent of the Calderon administration from the outset to address it.

From our perspective, the concern is the violence coming north of the border. From our perspective, we have seen and had several years ago an uptick in kidnappings of individuals who may live in the United States but have businesses or family be kidnapped in Mexico and the ransom sought from persons in the United States. We put together task forces to address that, and that has been reduced somewhat.

We have a priority of looking at corruption along the border, and we have a number of agents looking at border corruption. We have had a number of cases of border corruption that we have successfully investigated.

We have put together fusion squads or individuals who are familiar with corruption, familiar with the narcotics trafficking, white-collar crime, money laundering and the like in the squads that we are using—"hybrid squads" we call them—to address the activities on the border. And, finally, we have put together an intelligence capability down in El Paso that brings in the intelligence from each of our offices as well as from our legal attache in Mexico City and headquarters. And we integrate that with the other players that are working on the border.

Senator GRAHAM. Would you said it would be a fair observation that securing our border is probably more important than ever, that criminal activity is growing and that terrorism threats are growing, and that we should really look at securing the border as a national security imperative?

Mr. MUELLER. I think securing the border has always been a national security imperative, yes, sir.

Senator GRAHAM. But it seems to be even more so from your testimony.

Now, you mentioned something in your testimony that you should maybe ask hard questions, and I think that is probably good advice for us all. When it comes to *Miranda* warnings, is it the FBI's view that *Miranda* warnings are required for interviews that involve intelligence gathering for national security purposes?

Mr. MUELLER. If there is no intent to utilize the results of those interviews in a courtroom and the purpose was gathering intelligence, yes, it would be—and that happens all the time, particularly overseas.

Senator GRAHAM. Is it fair to say that homegrown terrorism is on the rise?

Mr. MUELLER. Yes.

Senator GRAHAM. Is it fair to say that we need to get our laws in shape to deal with a new threat, which is people attacking us who may be American citizens themselves who are here legally?

Mr. MUELLER. Yes.

Senator GRAHAM. So wouldn't it be fair to say that we should as a Nation, the Congress and the administration, try to find a solution that would withstand court scrutiny to deal with the fact that when we are facing this threat, providing a lawyer and reading someone their rights when they may involve an act of terrorism is something that may be counterproductive at the time?

Mr. MUELLER. I am not certain I could go that far. I would say we are bound by what the Supreme Court has issued in terms of——

Senator GRAHAM. Well, do you think Congress should be involved in helping create a solution to this problem?

Mr. MUELLER. It would be nice if Congress could, but we have got the Supreme Court as the ultimate arbiter in terms of the application of *Miranda* to the admissibility of statements, as I am sure——

Senator GRAHAM. I totally understand what you are saying, but it is my view that *Miranda* warnings are not required if the purpose of the interrogation is to gather intelligence about existing threats or future threats, because when you fight a war, you do not read people *Miranda* rights on the battlefield. Where is the battlefield? Is the United States part of the battlefield?

Mr. MUELLER. One can speculate. I know there are persons who say everything is a battlefield now. I would stay——

Senator GRAHAM. Well, what do you think?

Mr. MUELLER [continuing]. Away from speculating on the battlefield. I know where you are going, but I will stay away from the definition of battlefield.

Senator GRAHAM. In all fairness to you, I think it is pretty important to know where the battlefield is. To me, the battlefield is here at home. We have caught people who are trying to blow us up that are connected with people in Pakistan, allegedly. So, Mr. Director, I think home is the battlefield, and we need to craft solutions in light of this growing threat, and I look forward to working—and I would urge the administration to come to Congress to see if we can work together.

But under your policy guidance, this memorandum, how long can you hold someone without reading them their *Miranda* rights? If you catch someone here in America, an American citizen whom you suspect of being involved with al Qaeda or some foreign entity, a terrorist group, how long can you hold them without reading them their rights? How many questions can you ask them? And when do you have to present them to court?

Mr. MUELLER. Well, generally, within 24 to 48 hours one has to make the presentment to court, at which point in time they will be read their *Miranda* warnings. It depends on where you might be. It may be longer if you are not that close to a magistrate.

Senator GRAHAM. Well, let us continue to ask the hard questions. So under the policy, under the problem with presentment to court, you are talking about 24 or 48 hours. Is that enough time to gather intelligence?

Mr. MUELLER. It may well be. In certain cases we have——

Senator GRAHAM. Could it well not be?

Mr. MUELLER. It could not be.

Senator GRAHAM. Yes, I mean, you might actually want to call foreign intelligence services and see what do they know about this guy. You would certainly want to call the CIA. You would want to call the DOD, and you would want to make a good assessment.

I think the honest answer is that presentment and *Miranda* warnings need to be looked at anew in light of the domestic—in light of homegrown terrorism, and that is just my view. And I want to invite the administration to be a good partner on this, but I just feel like we are less safe with the current policy because the questions I have asked about how long you can hold them, 24 to 48 hours, without a presentment problem is probably not a good solution to what I think is a growing problem.

The last thing I want to ask you about is your budget. We are having a real debate up here about, you know, cutting Government, and God knows it needs to be reduced. But one thing about Government from my point of view is the first thing you want to do is protect your citizens. You are telling me that H.R. 1, if implemented the way it is today, would cost 1,100 job slots?

Mr. MUELLER. We would not be able to fill 1,100 slots by September in order to meet the budget constrictions.

Senator GRAHAM. So when we are deciding what is the right number to pick—you are losing $200 million. Is that correct?

Mr. MUELLER. Yes, we are.

Senator GRAHAM. And the plus-up you are asking in 2012, is that really——

Mr. MUELLER. Depending on what happens in 2011——

Senator GRAHAM. Right.

Mr. MUELLER.—will dictate to a certain extent the plus-ups in 2012. And what we are struggling for is to get what we did not get in 2011 for 2012.

Senator GRAHAM. Well, you know we are deeply in debt, right?

Mr. MUELLER. Absolutely. Absolutely.

Senator GRAHAM. I thought you might agree with me there. And you have looked at this budget from a perspective that the Nation is deeply in debt?

Mr. MUELLER. Yes.

Senator GRAHAM. And you are telling us, the Congress, that due to the threats that are multiplying exponentially you need this force to protect America?

Mr. MUELLER. Yes.

Senator GRAHAM. Thank you very much for your testimony.

Chairman LEAHY. Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman, and I want to thank you, Director, for your service. You started a week before 9/11, and it has been quite a decade. But thank you. You have done an excellent job.

Mr. MUELLER. Thank you.

Senator SCHUMER. I would like to discuss first an issue that affects a small upstate community, Newburgh, New York. As you know, 2 years ago Newburgh saw gang activity and a violent crime spike. There were shootouts in the streets, repeated bank robberies, numerous homicides. At the time you and Attorney General Holder assured me the FBI and other Federal partners would work closely with local law enforcement and significantly increase Federal resources to counter gangs operating in the area, and you have done a good job on that. Last spring, this work led to an FBI investigation, a multi-agency sweep involving some 500 local, State, and Federal law enforcement agents and the arrest of 70 gang members in the city of Newburgh. It is not a large city, so that was very significant.

Early last month there was another sweep, ten more gang suspects were arrested, and there have been reports now that the FBI is considering moving its Hudson Valley resident agency to Newburgh. I want to personally express my strong support of such a proposal.

When I toured the streets of Newburgh with the local police department and your field agents, residents thanked the officers and agents and saw hope. As the community works to rebuild, I know that housing the FBI within the community will serve as an important gang deterrent, an important community resource.

So can you commit to consider Newburgh closely as the location for the FBI resident agency location?

Mr. MUELLER. I think I can make that commitment. I know the decision is in process and that the activities in or about Newburgh would be a factor, amongst other factors as well. But certainly we would consider the activity that you have adverted to over the last year or two in terms of where that resident agency should be located.

Senator SCHUMER. OK. And if you are having any space problems, we will find it for you. OK? But it is very important to move there.

Mr. MUELLER. I understand.

Senator SCHUMER. So I hope you will do everything you can to do that.

Mr. MUELLER. Sure.

Senator SCHUMER. OK. The second question deals with the background checks pilot. In 2003, Congress passed the Criminal Background Check Pilot Program as part of the PROTECT Act. The legislation was introduced by Senator Hatch, cosponsored by a number of Senators on the Committee. I was one of them. This pilot

program was established to determine the feasibility of a nationwide fingerprint-based background check system for volunteers of youth-serving organizations like the Boys and Girls Club, the National Mentoring Partnership. Thanks to the great work of the FBI and the National Center for Missing and Exploited Children, which processed background check requests, some 90,000 records have been requested and used since this pilot program's inception. Six percent of the records included criminal histories of concern, including serious offenses, sexual abuse of minors, assault, child cruelty, even murder.

So, Director Mueller, has the FBI experienced any problems in running these checks for these youth-serving organizations? For instance, does the FBI believe the costs associated with this pilot program to be overly burdensome or the work overly complex?

Mr. MUELLER. My understanding is that there has been no problems with the processing of these requests through NCMEC. NCMEC is a tremendous organization. So we have not seen any problems, and I do believe that the charges that we—what we charge for is an appropriate charge, and my understanding is there have been no problems in terms of receiving the monies for those checks.

Senator SCHUMER. OK, because as you know, NCMEC recently announced it would no longer operate the pilot program, leaving a number of youth service organizations without access. So given the Bureau's experience with the pilot, do you agree such a permanent program could be helpful in the continued protection of our children? Are you willing to work with whatever organization takes NCMEC's place?

Mr. MUELLER. We would take directly from those youth service organizations the requests for doing the background checks.

Senator SCHUMER. Good.

Mr. MUELLER. And, consequently, I probably cannot say to what extent that going back to that practice would be detrimental to those organizations or others.

Senator SCHUMER. But you are willing to work and make sure that this gap is filled again because it is a worthwhile——

Mr. MUELLER. If there is indeed a gap, yes, we are willing to work with NCMEC or youth service organizations in order to make certain that the processes undertaken——

Senator SCHUMER. Great. OK. Finally, guns, gun checks. The President himself has noted information included in our gun check system, NICS, which is supposed to prevent guns from being sold to the wrong people, is "often incomplete and inadequate." The FBI relies on State governments to supply many of the records about people who are not allowed to possess guns, and there are lots of examples of this: people who are involuntarily committed to a mental institution by a State court, someone on probation for a State crime fails a drug test. And yet we are finding that many States are not complying.

So you have any idea why so many States are not doing anything to help you enforce the Federal law in this regard, why we are not getting the information that we should to be on this list? Which, by the way, everyone supports. This is not about who should own a gun. This is once there is a consensus that say a felon or some-

body who is adjudicated mentally ill not get a gun, that they be on the list so they will not be sold a gun.

Mr. MUELLER. We do everything we can to encourage the States to provide us the information that would be present in NICS that would prevent the sale of those particular guns. I do not think there is one particular factor that contributes to the inability or unwillingness of a State to provide that information. It may well be it costs additional time and money to ferret out that information and put into place a process to assure it goes into NICS. All we can do in the Bureau is encourage that the States provide us that information.

Senator SCHUMER. Well, you could just send us things we might be able to do now. As you know, I have been working on legislation on this for a long time. Representative McCarthy and I passed legislation about the mentally infirm, adjudicated mentally infirm, after Virginia Tech. Recently, Jared Loughner, the Tucson gunman, was rejected by the army due to his admitted drug use. Under the bill that McCarthy and I have put in, under Federal law, it seems to me such information could have been sent to NICS under existing law.

So given that the President has stated that the NICS Improvement Act has not been properly implemented and Loughner's ability to purchase a firearm even after admitting to the Federal Government—this is when he was applying to the armed forces—about his drug abuse, will you agree to examine the implementation of this legislation to ensure it is serving its intended purpose, for instance, having the armed forces report to NICS in these types of instances like Loughner?

Mr. MUELLER. As I say, in every one of these instances we encourage, but we have no ability to do much more than encourage the responsiveness.

Senator SCHUMER. OK. And can you provide me with updated numbers in the next few days on how many people have been identified as drug abuses by each Federal agency?

Mr. MUELLER. I think we can.

Senator SCHUMER. Great.

[The information appears as a submission for the record.]

Senator SCHUMER. Thank you, Mr. Chairman. My time has expired.

Chairman LEAHY. Thank you, Senator Schumer.

Senator Sessions.

Senator SESSIONS. Thank you, Mr. Chairman.

Director Mueller, thank you for your service. You came to this office with unparalleled experience, the proven judgment, and integrity to lead the agency in an effective way. I believe you have done that. I salute you for it. The country has been lucky to have you there. I have worked with the FBI many, many years and have the greatest respect for the men and women who serve in that fabulous agency, truly I think it is fair to say the greatest law enforcement agency in the world. Would you agree?

Mr. MUELLER. I cannot dispute that.

Senator SESSIONS. I did not think you would, not perfect——

Chairman LEAHY. We would have some problems if you did, Director.

[Laughter.]

Senator SESSIONS. It may not be perfect, and none of us are, but it is a great institution with fabulous men and women who serve every day, long hours and doing the things that are necessary to help protect us from crime and terrorist activities.

I would like to follow up a little on Senator Graham's questions about the *Miranda* warnings and the nature of the struggle that we are in with terrorism today. I remain totally baffled by this administration and, frankly, your perception that those who are dedicated to the destruction of this country, who enter our country with the design to attack and kill Americans somehow should be presumptively treated as criminals and should be provided *Miranda* warnings and other legal protections that we provide American citizens, but the kind of things that have never been provided to enemy combatants on the battlefield.

First of all, I want to just make clear that I do not think it is speculative about where the battlefield is. I think the battlefield is where the enemy is attacking us. And we have seen that they are attacking us in our homeland.

So I guess my first question is: How do you feel about the fundamental question of the apprehension of someone directly connected to al Qaeda in the United States bent on attacking the United States? Do you believe that should be treated as an act of war or a crime?

Mr. MUELLER. I am going to leave that up to others to decide. I will tell you that we as an organization, if the responsibility given to us under the law is to make the arrest and there is an intent and a decision made by the President, whichever President it may be, whether it be Bush before or Obama now, that the person go through the Federal district courts and the procedures are mandated that we go through in order to have testimony admissible in a courtroom.

Now, a decision can be made by the executive that they not go through the Federal criminal process of the United States, which is a decision to be made by the executive at whatever point in time, and that——

Senator SESSIONS. Well, I would agree——

Mr. MUELLER.—different procedures kick in. But if we are given the mandate to do the arrest and take them to trial and convict them under our courts, then there is a pathway that has been decided by the executive that we must follow.

Senator SESSIONS. Have you made a recommendation that that is the way, the presumptive way——

Mr. MUELLER. I have not. No, sir.

Senator SESSIONS. Have you opposed that?

Mr. MUELLER. That is an issue that is left to the President, and——

Senator SESSIONS. Decided at a level above you?

Mr. MUELLER. Way above me, yes, sir.

Senator SESSIONS. Well, I do not know, you being a long-time appointment, so you can speak candidly about what is important to protecting the safety of the United States of America. And you are not just expected to come here and rubber-stamp what decision is made in the White House. But according to the document you put

out on custodial interrogations, you say that the FBI policy, you will continue to adhere to the FBI policy regarding the use of *Miranda* warnings for custodial interrogations of operational terrorists. And you define operational terrorists as an arrestee who is reasonably believed to be either a high-level member of an international terrorist group or an operative. It goes on to describe that.

So let us take the situation that Senator Graham was asking you about, and I think it is very important. If this is an enemy combatant, and I believe many of these terrorists are, associated with al Qaeda or organizations committed to the destruction of the United States, then they should be seen as a potential source of intelligence information that could help us identify who else may be in this organization, who else is threatening the United States. And isn't it possible that you can obtain that kind of information through effective interrogation techniques?

Mr. MUELLER. Well, I agree with you, it is absolutely essential in our first—when we have individuals who are involved in terrorist attacks, our first objective is to obtain the intelligence. And what our guidance is to our persons is that should be your objective——

Senator SESSIONS. Well, that is——

Mr. MUELLER.—give advantage——

Senator SESSIONS.—your objective, but you indicate that there is some potential window of public safety exception which is not clear in any case law that I am aware of, not really clear what this public safety is. As you indicated, it cannot exceed 24 or 48 hours when they have to be brought before a Federal court if you are treating them as a criminal, right?

Mr. MUELLER. Well, if they are going to be treated in the courts of the United States——

Senator SESSIONS. How many hours——

Mr. MUELLER.—the requirement——

Senator SESSIONS.—has a court ever approved——

Chairman LEAHY. Let him finish.

Senator SESSIONS. Well, my time is about up, Mr. Chairman. It is an important issue.

Chairman LEAHY. He has answered these questions several times already, but I would like to let him answer——

Senator SESSIONS. I would like to get a square answer out of it, too.

Mr. MUELLER. And I am happy to answer.

Senator SESSIONS. Well, first of all——

Mr. MUELLER. Let me just say——

Senator SESSIONS. Let me just say to you——

Mr. MUELLER.—it is important to——

Senator SESSIONS.—this, and I will let you answer further. I believe that an individual arrested carrying a bomb, about to board an airplane in the United States directly connected to al Qaeda should be treated as an enemy combatant, does not need to be taken to court in 24 or 48 hours and given a lawyer, does not need to be given *Miranda* rights, may need to be subjected to weeks of interrogation utilizing the best information and techniques we have to find out who else in this country may be prepared to kill thousands of American citizens. And for you to say—and not acknowl-

edge that *Miranda* warnings can be counterproductive to that is inexplicable to me. So I would be glad to hear your comments.

Mr. MUELLER. Well, I have not exactly said that, Senator. What I have said is that if a person is arrested—may I finish? If a person is arrested in the United States under our laws, we are guided by the statutes and by the Supreme Court in terms of what we can do. We have expanded and identified what we anticipate we should get when a terrorist has been arrested in the United States in terms of intelligence, and that is the first thing, without *Miranda* warnings, we do. But ultimately if that individual is to be prosecuted in the United States, there may well come a point in time where *Miranda* warnings are warranted.

If the decision is made that the person is not going to go through our courts, that is a decision that is made by the executive and we quite obviously would follow that. But that person would not be in our custody or going through what we do day in and day out under the criminal justice system of the United States.

Senator SESSIONS. How long do you wait before you give a *Miranda* warning under an exception?

Mr. MUELLER. Under the exception? It is indeterminate. And we have had a number of occasions where we have put off both the giving of *Miranda* warnings as well as presentment for a number of days where we have got the person and the person agrees that they want to cooperate——

Senator SESSIONS. Well, they agree——

Mr. MUELLER.—and provide intelligence for a period of time.

Senator SESSIONS. They agree.

Chairman LEAHY. Thank you.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Director Mueller, I would like to associate myself with all the other Senators who have commended you for your service. Thank you so much.

I would also like to commend you for aggressively investigating mortgage fraud and predatory lending cases. Recently I became Chair of a new Subcommittee on Privacy, Technology, and the Law, and one thing I learned as I have been preparing for the Subcommittee's work is that at the height of the subprime lending crisis in the summer of 2007, the No. 1 buyer of Internet advertising across all industries was a subprime lender. This was a company called Low Rate Source. Another top-five Internet advertiser in this period may sound more familiar—Countrywide Financial.

And, Mr. Chairman, without objection, I would like to add the Nielsen net ratings reports to the record.

Chairman LEAHY. Without objection.

[The information referred to appears as a submission for the record.]

Senator FRANKEN. My point here is that subprime mortgages did not assign themselves, and one of the key ways that Countrywide Financial and other subprime lenders identified their targets was by gathering data about those customers online to see who might be a good mark and targeting them online, often without the customers' having any idea that this was happening. Is this a trend

that the FBI has seen during its investigations of subprime lenders?

Mr. MUELLER. I am not familiar myself with that. I would have to get back to you on it. But we can do that.

Senator FRANKEN. Well, Mr. Director, it seems to me this is an area in which the FBI would be well served by working with the Federal Trade Commission. Can you tell me what you are currently doing to work with the FTC on this issue?

Mr. MUELLER. Again, I would have to get back to you on it.

Senator FRANKEN. Thank you.

Mr. MUELLER. I know we have a number of task forces and working groups with them, but I would have to get back to you with the specifics.

Senator FRANKEN. I appreciate that.

[The information referred to appears as a submission for the record.]

Senator FRANKEN. A while back, I saw Representative Peter King, Chairman of the Homeland Security Committee in the House, say on TV pretty categorically that there was no cooperation from the Somali community or from community leadership in Minnesota after a very small number of members of that community went to Somalia to train with Al-Shabaab. My experience is that no one is more upset about what happened than the Twin Cities Somali community itself, and my understanding from talking to law enforcement is that there has been real cooperation from the community in Minnesota. Is that your understanding?

Mr. MUELLER. Yes, sir. I think that the Somali community in Minneapolis was taken aback by the number of young men who had traveled to Somalia to work with Al-Shabaab, and that that community, understanding what had happened to that community and the threat to the young men in that community, became very cooperative in terms of not wanting that to happen again.

Senator FRANKEN. Yes, that was my understanding. He said quite categorically the opposite was true, and I take umbrage on behalf of the Somali community in the Twin Cities whom I represent.

Now, it seems to me that it would make sense to have a Somali face on some of our counterterrorism efforts in the Somali community in Minnesota. Are you actively working to encourage and recruit members of key communities like the Somali community to actually become field agents?

Mr. MUELLER. Yes, we are. We have not been as successful as we would like, but we continue to press hard and recruit from all segments of the community.

Senator FRANKEN. Thank you.

Many incidents have come to light recently of banks and debt collection agencies fraudulently signing affidavits. This has likely resulted in wrongful foreclosures and in consumers paying thousands of dollars in money that they do not owe. In fact, Lori Swanson, Minnesota's Attorney General, filed a suit just yesterday against a large debt collection company alleging that it improperly signed hundreds of affidavits without verifying information. This has reportedly resulted in situations like that of a woman from Eagan, Minnesota—a southern suburb of the Twin Cities—who was pur-

sued for years—a bill that she had already paid on time. She repeatedly sent her canceled check as proof of payment to the debt collector, but it took her a very long time to finally get the case dismissed by a court, and she has never been able to repair her credit.

Do you think existing penalties for this type of fraud are strong enough? What more can we be doing to deter this kind of activity since it is so hard to make the victims whole after they have been defrauded?

Mr. MUELLER. First, I would have to give some thought as to what additional legislation is necessary, whether it be enhanced penalties in a particular area. I can tell you that we have a number of investigations going into this general area, and we have found that with the success of these investigations, we do have indictments and persons do go away for a substantial period of time. I am not familiar with this particular case, and so I cannot say whether those activities in that case are under investigation. I could not anyhow, but I can assure you we have a number of investigations.

Senator FRANKEN. Do not tell me anything I should not know.

As you know, I have been very interested in how mortgage fraud has affected Minnesota. After our last oversight hearing, I submitted a question for the record asking you to explain the process by which the FBI chooses to prioritize resources for mortgage fraud cases. You said the FBI addresses the most prolific schemes that have the greatest impact on the communities where the fraud has occurred.

I want to follow up on this because Minnesota has not just been affected by really big fraud cases. We have been hit by smaller frauds, too, where someone comes in and offers to refinance someone's home loan, gets all of the homeowner's information, then just steals the check when it arrives. Do you have the resources you need to investigate these smaller schemes and not just the highest-profile ones? And how are you working with state and local law enforcement to ensure that these outrageous cases of fraud are being prosecuted?

Mr. MUELLER. Well, what we endeavor to do is to work with State and local law enforcement in the form of either task forces or working groups, and we have currently 94 of these task forces and working groups around the country. We have almost 340 agents doing this. Probably we could use some more, but we do do a triage across not just the universe of cases in the Federal arena, but also with State and local law enforcement to see if we can get resolution of all the cases across the board. And so we will sit down with a working group and say, OK, how can this case be best addressed. Some will go to Federal court. Some will go to State court to be handled by district attorneys and the like. But our endeavor is to identify the universe and make certain that we get all cases that we can addressed in some way, whether it be at the Federal level, State or local, and that requires the coordination with State and local law enforcement.

Senator FRANKEN. Thank you. And, again, thank you for your service. I hope your next job is slightly less pressure, but I do want you to keep serving our country, and I know you will in whatever way you choose.

Mr. MUELLER. Thank you, sir.

Senator FRANKEN. Thank you.

Chairman LEAHY. Thank you very much, Senator Franken.

Senator Kyl.

Senator KYL. Thank you very much.

Director, I want to add my voice to those who have thanked you for your service. We appreciate it very much and obviously do wish you well. I would note, though, as in my case, your job is not quite done. I asked the Chairman if we might be calling you up one more time before you left. He said probably not, but I would not hold your breath yet.

Mr. MUELLER. I am with the Chairman.

[Laughter.]

Senator KYL. Let me first just follow up on a question that Senator Franken asked. The FBI does rely on the cooperation of the Muslim community to investigate radicalization particularly of young Muslims in the community. Is that not correct?

Mr. MUELLER. True.

Senator KYL. And I gather it would not be helpful to your efforts if members of the Muslim community refused to even talk to FBI agents without having their lawyer present.

Mr. MUELLER. I would state at the outset everybody in the United States has a right to have a lawyer present, but what we would like and ask of these communities is that they encourage their persons to cooperate with us and provide us the information, the tripwires that will help prevent the next terrorist attack.

Senator KYL. So it is not particularly helpful if they are advised that they do not talk to you unless they have a lawyer present?

Mr. MUELLER. I am familiar with one of the placards that one entity had there, which across the board urged persons not to talk to the FBI. And that is not contributions we want from our citizens to stop crime, stop terrorist attacks.

Senator KYL. Any citizen, for that matter.

Mr. MUELLER. Any.

Senator KYL. Right. Let me ask you about—could you describe just for the record in about 20 seconds what your Team Telecom mission is?

Mr. MUELLER. Team Telecom.

Senator KYL. Well, as I understand it, you have stood up a mission which assists in the evaluation of cyber activity by foreign corporations, for example. Maybe I should set the stage. I was just trying to set the preliminary stage. You are familiar with the Chinese companies Huawei and ZTE?

Mr. MUELLER. Yes, sir.

Senator KYL. And there are a couple specific things that your Team Telecom has been advised. Maybe you have a different name for it.

Mr. MUELLER. We call it CFIUS. I understand the process whereby the Government looks at the purchase of companies by——

Senator KYL. Right, and the FBI has a specific group that assists in that.

Mr. MUELLER. We do. We call it CFIUS. Yes, we do.

Senator KYL. Okay. One of the things that has been reported is that our country's sixth largest cellular provider, U.S. Cellular, is

contemplating having Huawei build out its 4g network. Now, given the fact that we were concerned enough about Huawei's potential contracting with AT&T and Sprint to the point that we intervened and both of those companies separated themselves from Huawei and did not move forward, what would your concerns be about such a contract with U.S. Cellular?

Mr. MUELLER. Well, this is something I am not certain we can address in open session. I can tell you the process is while we do not sit at the table with those who are in the CFIUS process, our recommendations or advice is often elicited, and we would do that in a classified setting.

Senator KYL. And the kinds of advice that the FBI would give would be based upon just hypothetically what kind of a concern?

Mr. MUELLER. Well, concerns that—speaking generally, not about one company——

Senator KYL. Just generally, yes.

Mr. MUELLER [continuing]. Or one particular process, but the concerns that through entities are operating with the backing of the Government that foreign governments may have access to classified communications to our intellectual property through proxies, and so the process, the CFIUS process, has been set up to assure that that possibility is examined, looked at, and a determination made as to whether or not a particular purchase of a company should go through.

Senator KYL. Right. One of the things that has occurred, at least we understand, that Huawei has partnered with the company Hibernia to help build and deploy a cable from New York to the U.K. that will transmit sensitive data including market information from the New York Stock Exchange. And I am curious whether or not your team CFIUS or Team Telecom has reviewed that partnership with Hibernia and the cable license involved with this cable landing and whether you could inform us about any considerations that you would have there.

Mr. MUELLER. At the outset, I am not familiar with the facts of that, but even if I were, I do believe it is the type of subject that would be addressed in a classified setting.

Senator KYL. Okay. Just so folks that might not be quite as aware of this would understand, a little bit of background. This firm Huawei has a background with the People's Liberation Army of China, is supported strongly by the Chinese Government, and at least in the past concerns have been raised about its involvement in the U.S. network, and that is the reason for the questions.

Would you have a concern about FBI systems being integrated or having Huawei, for example, being integrated into FBI systems?

Mr. MUELLER. I cannot speak to a particular company. I can say that ourselves, the intelligence community, are always concerned about assuring the security of our systems and the persons that are working on our systems or providing the capabilities that support our systems.

Senator KYL. Would that also include even down to the local level? In other words, any network that might carry sensitive information or be connected with one that would carry sensitive information would potentially fall within the mission of the FBI taking a look at it. Is that correct?

Mr. MUELLER. It may well be that in those circumstances we would take a look at it. If you are talking about our systems, we would always be concerned about trap doors or back doors and ways into our systems. If there is a business purchase at some point, we may be asked to look at the impact of that purchase?

Senator KYL. Just generally speaking, is there anything that you would ask of us at this point? Or could I just ask you to perhaps think about that and supply for the record any recommendations or suggestions you would have about assistance that Congress could provide for you to do your part of this mission?

Mr. MUELLER. Yes, sir. Would be happy to.

Senator KYL. Great.

[The information appears as a submission for the record.]

Senator KYL. And then just one last question. One of the things that has been on going with the FBI and the Department of Homeland Security has been the matter—I am going back to the terrorist issue—of lexicon, and there is one theory that says you do not call people jihadists or Islamists because that simply gives credibility to their ideological foundation for their action. The other school of thought says if we are going to defeat a terrorist enemy, we need to at least be able to call it by its true name, understanding its etiology, its motivation of the people, what makes it tick so that we can effectively deal with it.

Where does the FBI come down in this matter of terminology?

Mr. MUELLER. Well, we call it as we see it. I understand that there is some discussion out there, but nobody has ever told us how we are supposed to describe terrorists or terrorist groups, and we try to give the most clear definition, but call it what it is.

Senator KYL. Would you agree that one accurate description of some of these groups like al Qaeda, for example, is Islamist?

Mr. MUELLER. Islamic extremists, absolutely.

Senator KYL. OK. Thank you very much.

Mr. MUELLER. Extremists. "Extremists" is an accurate definition.

Senator KYL. Just to be crystal clear, nobody is suggesting that the Muslim faith is responsible for all of this. But in the name of their view of their faith, a lot of folks—maybe not a lot, but a number of young people have been radicalized, and radicalized to extreme actions I guess is the reason for the extremist. But there is no denying the connection, in their mind at least, to their Islamist faith, I gather. Would you agree with that?

Mr. MUELLER. Agreed, yes.

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

Chairman LEAHY. Thank you, Senator Kyl.

Senator Coons.

Senator COONS. Thank you, Mr. Chairman.

Director, thank you so much for your testimony today and for your service to our country and for your diligent stewardship of the FBI. I have a number of areas I would like to touch on.

First, in my former role as a county executive, I had responsibility for a county police department, and hopefully we will be focusing some latter this summer on the Federal and local law enforcement interface and collaboration. The FBI is an enormous source of valuable intelligence, not just in the national security

area, in the anti-terrorism area, but also just in routine local law enforcement—drug interdiction, violent crime, and so forth.

Could you just comment on successes and areas of improvement for FBI intelligence sharing with local law enforcement and how you feel local law enforcement is doing nationally at moving toward intelligence-based policing?

Mr. MUELLER. Let me start with the information sharing. One of the great successes, I think, since September 11th is the growth of the Joint Terrorism Task Forces and that concept, and to the extent that we have been successful in cases, virtually all of them have been utilizing the combined resources of the FBI and other Federal agencies and State and local in the context of the Joint Terrorism Task Force.

I am a great believer also in task forces across the board, whether it be mortgage fraud task forces or gang task forces, violent crime task forces, because it gives you the combined capabilities of the entities, but also gets everybody on the same page so those vehicles provide a sharing of intelligence.

Second, I would say we are doing, I believe, a lot better job of informing generally State and local law enforcement of what is happening in the terrorism arena. We will all be, however, beat to the punch occasionally by CNN, and that is just a factor of life in this day and age. But right now we put out bulletins almost immediately after something becomes public with regard to a terrorist attack to all State and local law enforcement across the country.

Fusion centers that are—I think there are 70-odd around the country now that also contribute to the sharing. On many of these, the majority of them, we have FBI personnel even though they are State entities that are participating. That contributes to the sharing as well.

There will always be some tension between ourselves and others, particularly when the information that we are utilizing is classified because it may come from the CIA or NSA, and persons who do not get that information are often frustrated. So there will always be that tension, but I think we have made substantial progress, and that is one of the pluses, positive aspects of what has happened since September 11th.

Senator COONS. And how do you address concerns about classified information access? What is your process or prioritization when you reach a tipping point and conclude that it is essential that local law enforcement have access to that information?

Mr. MUELLER. Well, any person who is assigned to a Joint Terrorism Task Force goes through a background check and gets a top-secret clearance. And so if you are State and local and you are on a task force, you have access to that which the agents sitting to your right and left have. Many police chiefs have also gotten clearances so that they can have access to—police chiefs or sheriffs, access to the information.

But it has been our position throughout that if a person is responsible for the safety of a particular community, classification should not stand in the way of getting the information they need to protect their community. If there is a threat to a particular—to Wilmington, Delaware, and——

Senator COONS. Thinking hypothetically.

Mr. MUELLER. Hypothetically. And the chief of police has not got a clearance but there is a potential threat, you will get the information on that. We will find a way to get it, because I firmly believe those persons who have the responsibility for security have the right to that information if there is an immediate threat.

Senator COONS. That is very helpful. Thank you.

One other area I have worked on in collaboration with our Attorney General is DNA testing. We have only one State lab, our Office of Medical Examiner, which, oddly, comes under our State Health and Human Services Department, is understaffed, overworked, has a significant backlog. This is a challenge in many different States staying on top of the developing technology. Now that everyone watches it on TV, every defense lawyer believes they are entitled to, you know, top-level DNA testing, and there are a significant number of convicted offender samples—thousands in our case—that have not been reviewed as well.

One possible solution to this backlog that was suggested to us was to allow private labs to do some of the backlog testing, but there is an FBI standard—I believe it is Standard 17—that requires that there be a full—essentially a public lab double-check for any work that is being done by a private lab before the FBI will accept the results. I just would be interested in whether you are doing anything to ensure that FBI regulations are not resulting in needless inefficiencies. Our Office of Medical Examiner identified that standard as one challenge that essentially made it not worth their time to engage with private labs to have them, at reduced cost and better speed, help them with their significant backlog.

Mr. MUELLER. Well, there is a quality control process, a technological review process that you are adverting to that is required that one go through before it is ingested into the data base. Over the last year this has been an issue. We know those who are pressing to avoid this, and it may be in certain circumstances a bottleneck.

To the extent that it has been, we are trying to reduce that and put into place more efficient capabilities to assure that that quality control can be done without slowing the ingestion of the new samples into the data base. But most people agree that there needs to be a quality control before the samples do go in the data base. So what we are trying to do and will continue to do is make that process more efficient to remove the time lags and make certain that—and all of us want to get it in as soon as possible, make certain that is done as efficiently as possible.

Senator COONS. Well, thank you. I appreciate your testimony about these questions.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much, Senator Coons.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Mr. MUELLER. Good to see you, sir.

Senator BLUMENTHAL. I want to join in thanking you for your service over the years where I have had the privilege of working with you as Attorney General of the State of Connecticut. And I know that the Attorneys General of the United States appreciate your working so closely with them and really in a very close part-

nership, and I particularly want to thank you for training and attracting the great men and women of the FBI who serve us so well day in and day out. And on that note, I just want to come back to the questions you answered about your budget.

The inability to fill those 1,100 slots in my view would be really a disservice to the FBI and severely disadvantage this great organization, and I hope you agree with me in that.

Mr. MUELLER. It would set us back. It is a setback, and we have been moving forward with the help of Congress and the Committee and the appropriators, and this would stall the progress that has been made.

Senator BLUMENTHAL. Thank you. You know, I want to commend the FBI for its focus on an area that I think is extremely important—anabolic steroids. Recently in Danbury there was a major set of arrests involving breaking a drug ring that was selling steroids to high school users in the Danbury area, selling 70 bottles each month of these steroids to so-called individual users. And I know that very often we focus on street drugs, and the DEA has a responsibility in this area. But I want to commend the FBI for its focus on the steroid problem, which sometimes receives too little attention or awareness. And I wonder if the FBI is planning additional efforts to combat the spread and use of steroids, particularly among young users, high school and college users around the country.

Mr. MUELLER. I would say this generally is not an area that we would, particularly in this time of budget constraints, spend a lot of effort on, particularly when the primary agency with the jurisdiction is DEA.

Now, we have become involved in investigations with DEA when steroids are coming from outside the United States with the Customs and Border Patrol, and we will contribute and participate in those investigations when we can provide something unique to further that investigation.

But beyond that, I would have to go back and see what we are doing and get back to you on that, but I cannot say that given the challenges that we have and the threats that we have that this would be as high a priority as all of us would like.

Senator BLUMENTHAL. Well, I know that you have enormous challenges, and some of them we have heard today. But I would be interested in your additional information and also increased participation and support for other agencies that may have a primary role in this area, because I do think that the spread of these steroids, indeed an epidemic of their use, and an acceptance of their legitimacy is one of the great threats to our young people today, and I appreciate your willingness to cooperate in that effort.

Mr. MUELLER. Thank you.

Senator BLUMENTHAL. On a subject that others have asked you about, the mortgage foreclosure issue, I have to confess that I am unhappy and frustrated with the most recent efforts by the administration to send a message in this area—the robo-signers, which are a subject of ongoing investigation by the State Attorneys General, which I helped to initiate. So far we have seen virtually no major actions by the task force that the President has appointed. In the face of blatant fraud on the court involving the robo-signers,

false affidavits, clearly in my view criminal violations that are a fraud on our justice system, and I wonder if you could respond, please.

Mr. MUELLER. Sure. I share that concern and belief that there is fraud out there, and I can tell you we have ongoing investigations.

Senator BLUMENTHAL. And I hope that we will see prosecutions soon. I do not want to put words in your mouth, but if you share my frustration, I hope that you also share my belief that we ought to have action soon.

Mr. MUELLER. I do not disagree with that.

Senator BLUMENTHAL. Thank you.

On the issue of missing children—and you have covered it a little bit—as you may know, the FBI was very constructively involved in a recent highly publicized search in the New Haven area for a missing 13-year-old, Isabella Oleschuk, who fortunately was found after 3 days. She appeared—in fact, left her own home on her own initiative, so she was not actually abducted or taken. But as you know, this problem is pervasive around the country. In Connecticut alone, the National Center for Missing and Exploited Children, a great organization that does wonderful work, received 67 reports of missing children in Connecticut last year, and 19 are still missing. And I know that the FBI has extraordinarily important other tasks, but I wonder whether this has taken increased—has come to be seen as a subject of increased priority in the FBI.

Mr. MUELLER. I would say it has always been a priority. When a child is lost, every special agent in charge wants to work with State and local law enforcement to find that child, and we will participate in the investigation so long as there is a Federal basis. And generally that is the thought being the person may well have been taken, abducted across State lines. There are occasions where we have to withdraw from investigations where the child has been found, and yet there is some investigative work to be done, but we have lost the Federal jurisdictional basis for it.

But I can tell you, when a child is lost, we as well as every other law enforcement entity around bring whatever we can to make certain that we find that child. We have experts—actually we have expert teams that are set up specifically to go to and address that circumstance when a child is lost.

Senator BLUMENTHAL. I welcome that response, and I would note that it marks a departure from many years ago when missing children were thought to be exclusively a local or State issue, and particularly now that many missing children are likely to be taken across State lines either by parents or others, I think that is a very commendable approach.

Mr. MUELLER. I can tell you that while not all missing children find their way to my BlackBerry, many of them do and we monitor that all the way up to the top.

Senator BLUMENTHAL. Well, I thank you very much, and, again, thank you for your extraordinary service to this Nation, and I think since I am the last questioner, I may enable you to leave this hearing unscathed and unwounded.

Thank you, Mr. Chairman.

Mr. MUELLER. Thank you. Thank you, sir.

Chairman LEAHY. Thank you, and my only concern is we have CALEA, the Communications Assistance Law Enforcement Act, which I helped draft back in the 1990's. We worked closely with the Bureau and everybody else because, as I recall, part of it I drafted in my hideaway office with others around. I hear concerns that it may go dark, and I just urge you and your office to work with me and others who do not want that to happen, to make sure that we can keep this going. May I have that assurance?

Mr. MUELLER. Yes, sir. Absolutely.

Chairman LEAHY. Thank you.

Okay. Well, I thank you very much. I appreciate you being here. I appreciate Attorney General Blumenthal wrapping it up, and thank you.

Mr. MUELLER. Thank you, sir.

[Whereupon, at 11:52 a.m., the Committee was adjourned.]

[Submissions for the record follow.]

QUESTIONS AND ANSWERS

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

December 6, 2011

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of FBI Director Robert Mueller at an oversight hearing before the Committee on March 30, 2011.

We apologize for the delay and hope that this information is of assistance to the Committee. Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Minority Member

Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the March 30, 2011, Hearing Before the Senate Committee on the Judiciary Regarding FBI Oversight

Questions Posed by Senator Klobuchar

1. Thank you for sending the FBI's Assistant Director of the Criminal Investigative Division, Kevin Perkins, to a hearing that I held recently on ways we can help law enforcement find missing children. I held this hearing after seeing an article in the New York Times which discussed a particular subset of kidnappings: family abductions.

According to a Department of Justice study, approximately 800,000 children are reported missing each year. That number is tragically high, but even more surprising is the fact that 200,000 of those cases are the result of family abductions, and approximately 12,000 of those cases last longer than six months.

The newspaper article pointed out that in many of these cases, the abductors continue to file federal tax returns where they continue to claim their child as a dependent, using their new address information.

In these cases, the Internal Revenue Service may unwittingly have more information about a missing child's location in its databases than law enforcement does. Yet the IRS doesn't currently have the authority to share that information with federal, state, or local law enforcement.

Can you comment on this issue? Do you think that giving the FBI additional tools to get information from the IRS in this small subset of cases would be useful?

Response:

Address and employment information, along with other contact, location, and identification information that the Internal Revenue Service (IRS) may have relating to an abducted or endangered child and/or to those responsible for abducting or endangering the child, can be of critical value. Experience shows that IRS records often contain this information, as well as information related to those who may have, or may have had, custody or control of such children or

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00039 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.002

knowledge of their locations. Although we understand there may be some concern that taxpayers will be less inclined to file tax returns if they know location information is provided to investigators attempting to locate missing children, we believe such a narrow use of location information is unlikely to have a broad effect on taxpayers generally and we would be pleased to work with the IRS and others to address these concerns. While the FBI uses the existing legal process to obtain court orders in appropriate circumstances, a streamlined process would enable law enforcement officials to obtain this critical information more quickly. The value of obtaining this information very quickly is great because time is critical when we are attempting to identify a child's location in order to secure the child's safe return. It is also critical that this information be disclosed in all cases of abducted or endangered children in which law enforcement requests are made to the IRS, regardless of whether the case is being investigated by federal, state, or local authorities (most child abduction or endangerment cases are investigated at the state or local level). We would be pleased to work with the Committee to develop appropriate legislation for this purpose.

In contrast to information relating to location and identity, as described above, the FBI currently does not seek, and sees no value in obtaining, financial information held by the IRS because financial information will not assist us in locating or recovering missing children. Consequently, legislation addressing this issue would not need to provide for the disclosure of financial information.

2. We have heard that because of new technologies and outdated laws, there is a growing gap in the FBI's ability to get court-ordered information from communications and internet service providers. In prior statements, you have referred to this as the problem of "going dark."

a. Can you tell us more about this "going dark" problem?

Response:

In order to enforce the law and protect our citizens from threats to public safety, the FBI must have the ability to intercept electronic communications with court approval. In the ever-changing world of modern communications technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications. We confront, with increasing frequency, service providers who do not fully comply with court orders or other statutorily authorized processes in a

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00040 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.003

timely and efficient manner. Some providers cannot comply promptly but are able to do so after considerable effort and expense by the provider and the government. Other providers are never able to comply fully.

The FBI calls this capabilities gap the problem of "Going Dark." As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence that it has legal authority to collect in a wide range of cases, including child exploitation and pornography, organized crime, drug trafficking, terrorism, and espionage. This gap poses a growing threat to public safety.

b. What do you need to fix this problem?

Response:

The President's FY 2012 budget requests approximately $15 million to establish a Domestic Communications Assistance Center (DCAC). The DCAC will serve as a hub for electronic surveillance knowledge management, facilitate the sharing of technical solutions and know-how among law enforcement agencies, advance initiatives to implement solutions that comply with the Communications Assistance for Law Enforcement Act, and strengthen relationships between law enforcement and industry. The FBI believes the DCAC will be a significant step forward in addressing the capabilities gap.

The Administration has convened an interagency working group to review the Going Dark problem and identify possible solutions. Any proposed legislation will be appropriately coordinated through the interagency process.

c. Some have suggested that efforts to solve this problem could create a "backdoor" to the Internet, or would give the government a "key" to the internet. Do you think that is a legitimate concern?

Response:

When the term "back-door access" is used, we believe it connotes surreptitious or clandestine access; in contrast, "front-door access" connotes access that occurs with the knowledge and assistance of the service provider. Back-door access, then, would occur if a system were entered and information removed without the knowledge of the system owner. Front-door access occurs when the provider

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00041 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.004

knowingly provides to the government the communications of the target in accordance with a court order or other statutorily authorized process.

Within that definitional framework, the current construct of the Communications Assistance for Law Enforcement Act (CALEA), Title III, and the Foreign Intelligence Surveillance Act presumes front-door access. Although there may be very odd fact patterns in which surveillance occurs without the knowledge of the service provider (for example, if the service provider is corrupt or is actively engaged in the criminal conduct under investigation), most of the time that the government is engaged in electronic surveillance of email activity, the service provider is actively engaged in effecting the court-authorized wiretap. The involvement of the service provider adds an element of privacy protection (for example, the service provider will receive and review a court order and configure the collection device to isolate the communications of the target to the exclusion of all others for delivery to the party conducting the wiretap). This construct has generally worked well through the years. While the FBI prefers that front-door access continue to be the norm, in order for that construct to be successful service providers must have available to them a technological means of effecting court-authorized wiretaps in a timely and efficient way.

3. I'm concerned that we're seeing an increased prevalence of certain kinds of "synthetic" drugs. Senator Schumer has introduced legislation to ban certain synthetic stimulants that are being sold as "bath salts," and Senator Grassley has introduced a bill to ban "synthetic marijuana." I'm a cosponsor of both bills because I think this is a really important issue – and tragically, a young man died in Minnesota two weeks ago after overdosing on a synthetic hallucinogen known as 2C-E, which I also want to see banned. Has the FBI noticed an increase in these types of drugs in its investigations?

Response:

The FBI does not typically conduct investigations regarding synthetic drugs because these drugs are not normally distributed by the high-level drug trafficking organizations commonly targeted by the FBI. Synthetic drug investigations are primarily conducted by the Drug Enforcement Administration and other agencies.

Questions Posed by Senator Franken

4. At the height of the subprime-lending crisis in the summer of 2007, among the top buyers of Internet advertising across all industries were Countrywide Financial and Low

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00042 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.005

Rate Source, two well-known subprime lenders. One of the key ways that these companies identified vulnerable borrowers was by gathering data about those customers online, without the customers' knowledge or consent. Has the FBI noticed or identified this trend during its mortgage fraud and subprime loan investigations? Please describe how the FBI has worked with other federal agencies, specifically the Federal Trade Commission, to combat this serious problem.

Response:

While the FBI does investigate mortgage loan origination fraud schemes, we do not specifically capture data regarding on-line behavioral targeting by subprime lenders. In addition, although we understand that on-line data mining and behavioral analytics are common elements of the marketing strategies of many financial services companies, the FBI has not identified general trends suggesting such practices were a key element of the scheme.

The Federal Trade Commission (FTC) is responsible for addressing consumer protection issues of this type, and the FBI works closely with our FTC partners regarding allegations of mortgage fraud, including allegations that a vulnerable population is being exploited by industry insiders. The FBI and the FTC are both members of the President's Financial Fraud Enforcement Task Force (FFETF), which was established in November 2009 to lead an aggressive, coordinated, and proactive multi-agency effort to investigate and prosecute financial crimes. FFETF participants include federal, state, and local law enforcement agencies, regulatory authorities, and inspectors general. Because it includes both criminal and civil enforcement resources, the task force is able to effectively coordinate efforts across the federal executive branch and with state and local partners. As a result, the U.S. Government (USG) is able to more effectively combat discrimination in the lending and financial markets, investigate and prosecute significant financial crimes, and recover proceeds for victims of these crimes.

5. During your testimony, you stated that the FBI continues to recruit field agents from all segments of the community, including members of the Somali community in Minnesota. Can you please describe in detail the FBI's recruitment strategy and efforts to recruit a diverse group of field agents, which includes members of the Somali community? Please specify what communities and geographic areas you are targeting for recruitment.

Response:

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00043 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.006

In recognition of the increased need for workforce diversity, the FBI has focused hiring efforts in various cultural heritage communities, including the Somali community. The FBI's Community Outreach Program (COP) has worked first to build trust and understanding in the community regarding the FBI's mission. COP coordinators have conducted recruitment activities in communities with large Somali populations, including in the following cities.

- Minneapolis MN
- Columbus OH,
- Kansas City, MO
- Seattle, WA
- Denver, CO
- San Diego, CA
- New York, NY

Recruitment activities include sponsoring traditional informational sessions at college/university campuses, Somali youth centers, career fairs, and during other community events. Because of the high concentration of individuals of Somali descent in Minnesota, many of those recruitment events involve direct contact with Somalis interested in FBI employment opportunities. While many Somalis express a strong interest in working for the FBI, they are often unaware of the available career paths and of the background/security requirements for FBI employment. Potential candidates are individually engaged in positive, honest dialogue regarding the FBI's hiring process, and qualified candidates are encouraged to apply. Qualified applicants for special agent and professional staff positions who possess the required level of Somali language proficiency are prioritized for hiring.

Media strategies used to communicate directly with the members of cultural heritage groups include advertisements in the following media when funding permits.

- Warsan Times monthly newspaper (statewide in Minnesota)
- Somali Link monthly newspaper (statewide in Ohio)
- Hiiran website (nationwide)
- The Linguist Society of America (nationwide)
- Minneapolis TV Network (Somali viewership in Minneapolis)
- Afrotainment TV (Somali viewership in New York City)
- SAR FM Radio (listeners in New York City)

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00044 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.007

In addition, focused collegiate recruitment events have taken place at the following schools.

- American University (Washington, D.C.)
- Cameron University (Lawton, Oklahoma)
- Michigan State University (Lansing, Michigan)
- University of Minnesota (multiple campuses)

The FBI is also working to increase its cadre of Somali contract linguists, participating in recruitment events that target Somali speakers in the following cities.

- Buffalo
- Chicago
- Honolulu
- Newark
- New York City
- Minneapolis
- San Francisco
- Los Angeles
- Minneapolis

The FBI looks to its contract linguists (all of whom have security clearances) as a key source of recruits for full-time, permanent FBI employment. We currently employ nine full-time Somali contract linguists, one part-time contract linguist, and two full-time language analysts. Nine additional Somali contract linguists have been placed in the background investigation process.

6. Why do you think the FBI's earlier efforts to recruit Somalis were less successful than intended? How has the FBI modified its recruitment strategy in light of lessons learned from those earlier efforts? What efforts has the FBI taken to encourage young members of the Somali community to pursue a college education so that they are eligible to become field agents?

Response:

The FBI has implemented grassroots strategies to inform and educate Somali communities regarding the FBI's interest in identifying and hiring qualified candidates from those communities. Recruitment and community outreach efforts at Somali youth and community centers, at high schools, and on college campuses

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00045 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.008

directly address the value of a college education in qualifying an applicant for FBI special agent positions and making a candidate more competitive for professional staff positions. Beyond education, the FBI is also continuing its efforts to increase awareness within Somali communities of FBI employment criteria related to U.S. citizenship, experience, suitability, and the background investigation process.

7. Please provide the following information regarding FBI criminal history record information (CHRI) checks for each of the past five years (2010, 2009, 2008, 2007, 2006):

a. The total number of CHRI checks generated for criminal justice and non-criminal justice purposes, including for both employment and licensing purposes, as well as the total number of CHRI checks that contained incomplete state criminal history record information.

Response:

Following are the numbers of fingerprint-based criminal history record checks for criminal justice and non-criminal justice purposes in the past five years.

Year	Criminal	Non-Criminal (Civil)
2006	10,549,254	12,563,812
2007	11,541,774	14,519,778
2008	14,039,182	21,471,570
2009	30,446,642	22,234,633
2010	37,559,659	23,695,415

The FBI does not collect information regarding the number of criminal history record checks that contain incomplete state criminal history record information.

b. Please provide detailed information about all incomplete CHRI records generated for non-criminal justice purposes, including the percentage and number of records that are incomplete broken down by state; the average number of missing dispositions on each CHRI report; the age of those incomplete arrest records (i.e. more than 1 year old; more than 5 years old; more than 10 years old, etc.); the nature of the offense (by major categories, such as felonies, misdemeanors, property crimes, and violent crimes); and the race of the subject.

Response:

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00046 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.009

The FBI does not collect the requested statistics regarding criminal history records generated for non-criminal justice purposes.

c. The total number of CHRI checks generated for employment and licensing purposes that include incomplete information not provided by the states, broken down according to the major sources of the requests (including, but not limited to, the Office of Personnel Management NACI checks; TSA port worker and hazmat driver checks; state laws authorizing employment and occupational licensing checks; FDIC authorized requests; PROTECT Act requests; long-term care requests; private security guard and aviation worker requests; and other requests authorized by federal statute).

Response:

The FBI does not collect the requested statistics regarding criminal history records generated for employment and licensing purposes.

8. For each of the past five years (2010, 2009, 2008, 2007, 2006), please indicate the number of "non-serious offenses" withheld from reporting for non-criminal justice CHRI checks pursuant to 28 C.F.R. §20.32(b).

Response:

Because state statutes and terminologies vary, the FBI requires each state to determine what is a serious or non-serious offense under its state laws for purposes of compliance with 28 C.F.R. § 20.32.(b). The FBI maintains records of the serious offenses submitted by the states and includes this information in the criminal history records disseminated pursuant to non-criminal justice checks.

9. For each of the past five years (2010, 2009, 2008, 2007, 2006), please provide the following information regarding public requests received to correct an incomplete or inaccurate CHRI:

a. The number of public requests.

Response:

Following are the numbers of requests from members of the public to correct incomplete or inaccurate records during the past five years.

Year	Number of Requests

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00047 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.010

2006	540
2007	1,180
2008	1,423
2009	1,234
2010	1,306

b. The age and types of offenses that generated these public requests.

Response:

The FBI does not collect information regarding the ages and types of offenses that generate public requests.

c. The number and percent of these CHRI records that were updated as a result of these public requests.

Response:

2010		2009		2008		2007		2006	
No. of Records Modified (60%)*	Total Modifica-tions Made**	No. of Records Modified (60%)*	Total Modifica-tions Made**	No. of Records Modified (60%)*	Total Modifica-tions Made**	No. of Records Modified (60%)*	Total Modifica-tions Made**	No. of Records Modified (60%)*	Total Modifica-tions Made**
784	5,278	740	4,824	854	4,273	708	no data	324	no data

*It is estimated that modifications to update and/or correct record information are made in 60 percent of the records challenged.

** These statistics include modifications that were not requested by the subject of the record, including requests by the contributing agency and discrepancies noted during review. There may be multiple modifications to a single record.

d. The number of staff assigned to these requests on annual basis.

Response:

Following are the staff assigned to these requests for the past five years.

Year	Staff Assigned

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00048 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.011

2006	8
2007	8
2008	8
2009	8
2010	9

e. The costs associated with this service.

Response:

The estimated annual cost to provide this service in Fiscal Year (FY) 2011 is approximately $600,000.

10. For each of the past five years (2010, 2009, 2008, 2007, 2006), please provide the following information:

a. The total number of NICS request received to conduct background checks on individuals purchasing firearms (also known as "Brady checks").

Response:

Following are the numbers of firearm background checks initiated through the National Instant Criminal Background Check System (NICS) for the past five years. (These statistics do not represent the numbers of firearms sold.)

Fiscal Year	
2010	14,088,406
2009	14,405,775
2008	11,808,254
2007	11,110,828
2006	9,712,348
Total	**61,125,611**

b. The total number of CHRIs generated for NICS purposes for each of the past five years.

Response:

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00049 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.012

The Interstate Identification Index includes millions of criminal history records. Every NICS transaction includes a search of this database. These transactions also include searches of the National Crime Information Center, the NICS Index, and, for potential firearm purchasers indicating foreign places of birth, the U.S. Department of Homeland Security Immigration and Customs Enforcement. A "delay" response on a NICS transaction indicates that information supplied on the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Form 4473 is a potential match with information contained in one or more of the databases searched by the NICS. The following statistics indicate the FBI transactions[1] that were delayed to permit further research by a NICS Legal Instruments Examiner (NICS examiner) during the past five years.

Fiscal Year	
2010	1,728,391
2009	1,780,836
2008	1,498,023
2007	1,391,061
2006	1,392,929
Total	**7,791,240**

c. The specific offenses that are disqualifying for NICS purposes.

Response:

Pursuant to 18 U.S.C. § 922 (t) (2), a licensed dealer may not transfer a firearm to any person unless the receipt of the firearm would not violate federal or state law. The NICS applies the federal prohibitors and any applicable state laws that prohibit firearm possession. Following are the offenses that are disqualifying under federal law.

- 18 U.S.C. §922 (g) (1) - Has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year
- 18 U.S.C. §922 (g) (2) - Is a fugitive from justice

[1] These statistics do not include transactions processed by Point-of-Contact states, as the FBI's NICS Section does not have access to that information.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.013

- 18 U.S.C. §922 (g) (3) - Is an unlawful user of or addicted to any controlled substance

- 18 U.S.C. §922 (g) (4) - Has been adjudicated as a mental defective or committed to a mental institution

- 18 U.S.C. §922 (g) (5) - Is illegally or unlawfully in the United States

- 18 U.S.C. §922 (g) (6) - Has been discharged from the Armed Forces under dishonorable conditions

- 18 U.S.C. §922 (g) (7) - Having been a citizen of the United States, has renounced U.S. citizenship

- 18 U.S.C. §922 (g) (8) - Is subject to a court order that restrains the person from harassing, stalking, or threatening an intimate partner or child of such intimate partner

- 18 U.S.C. §922 (g) (9) - Has been convicted in any court of a misdemeanor crime of domestic violence

- 18 U.S.C. §922 (n) - Is under indictment or information for a crime punishable by imprisonment for a term exceeding one year

d. The average number of incomplete offenses per NICS request that required additional information to be located from the state and local authorities.

Response:

The FBI's NICS Section began a concerted effort to collect missing disposition information in January 2009 with the implementation of a "Waiting for Disposition" (WFD) feature that allows us to track requests for disposition information. While our data indicate that in FY 2010 an average of 4.27 requests were sent out per delayed NICS transaction, not all WFD requests seek disposition information. Requests also concern police reports related to misdemeanor crimes of domestic violence, protection orders, mental health evaluations, and other information. Often, multiple agencies must be contacted to obtain one missing disposition, or a single transaction may include multiple dates of arrest for which final disposition information is needed.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.014

e. The average cost of searching for this incomplete offense information.

Response:

In calculating the cost of researching incomplete offense information, the data currently being captured cover the time period from the NICS examiner's receipt of the transaction (when the examiner begins research internally to locate the missing information) until initiation of the external request. The cost of updating the record once the information is received is not currently being captured. Based on the data available for FY 2010, the FBI estimates the cost associated with the examiner's research to be $6.9 million.

f. The total number of FBI staff designated to tracking down missing disposition information for NICS checks.

Response:

As of 3/31/11, the NICS Section has 370 NICS examiners on board whose primary responsibility is conducting the background checks related to firearms transactions. In addition to processing appeals from individuals who have been denied firearms purchases, these employees track down missing disposition information related to NICS transactions.

g. The number and percent of records where all offense information could be collected in the prescribed three-day time period.

Response:

During FY 2010, 693,755 requests for disposition information were sent to other agencies. While responses to 251,473 (36.25%) of these requests were received within the 3-day period, only a portion of these responses contained the information needed to make a final decision on the transaction (the FBI does not maintain statistics indicating the number of responses that were sufficient to reach a determination of eligibility). Of the 693,755 requests for disposition information, 100,699 (14.52%) of these requests received responses after the 3-day period and 341,583 (49.23%) received no response.

As noted above, transactions may require us to contact multiple agencies to obtain disposition information regarding a single arrest or regarding multiple arrest cycles. NICS examiners do not request information on every offense with a

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.015

missing disposition, but only on those that may disqualify a potential firearm purchaser. Once information is received from an external source allowing the NICS examiner to make a decision, the transaction is finalized even though there may be other requests outstanding.

11. Please provide the policies and procedures the FBI uses in the following circumstances:

a. The FBI's system for prioritizing its search for missing disposition information for NICS firearms checks.

Response:

The NICS Section prioritizes transactions that hit on warrants first, with other transactions being handled as they are received (the oldest transactions are processed first). The NICS Section's Standard Operating Procedure (SOP) mandates that all automated systems, including approved court web sites, be checked before calling or faxing an external agency to locate missing disposition information. Section 5.5.4 of the SOP requires the following "in-house" research before making external contacts.

- Perform a NICS Transaction Number inquiry to determine if other transactions exist on the same subject.

- Check the Disposition Document File (DDF) to determine if there are any matches to the subject. The DDF is a database containing over one million documents obtained from federal, state, local, and tribal agencies primarily through previous research relating to firearms and explosives transactions.

- Check any ATF Relief of Disabilities Database hits to determine if there is a match.

- Check the FBI's Integrated Automated Fingerprint Identification System (IAFIS) for disposition or to obtain a State Identification Number in order to search for state -held information.

- Check the National Crime Information Center.

- Check any relevant Internet web sites for final dispositions.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.016

• Use the NICS Section's Reference Library, including the following books.

  ○ The Felony Laws of the 50 States and the District of Columbia (1986).

  ○ State Law and Published Ordinances – Firearms.

  ○ Federal Firearms Regulations and Reference Guide.

  ○ State criminal codes.

• Use Westlaw to obtain offense levels or maximum sentence terms for specific charges.

• Contact the NICS Section's Legal Research and Analysis Team to clarify misdemeanor crimes of domestic violence, alcohol/drug charges, state prohibitors, federal charges, etc.

If final disposition information is not located during these searches, the NICS examiner will use "external research" (SOP § 5.5.5), which includes federal, state, local, and international contact lists to call, fax, or e-mail courts, state bureaus, arresting agencies, and other appropriate entities to obtain the necessary information.

b. The process the FBI uses to update its records once it receives current disposition information that is located as a result of the NICS contacts with state and local authorities.

Response:

The procedures used by the NICS Section to update criminal history records when the requested information is received are provided in SOP § 5.6.3, "Document Routing." Those procedures follow.

• Forward information to the NICS Support Unit to update criminal history records posted on IAFIS.

• Forward dispositions to states when only the state record can be updated.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.017

• Information that cannot be posted to IAFIS or updated to the state record will be automatically saved to the DDF.

• If an "arrest" record reflects a detention rather than an arrest, forward an expungement or partial expungement of the criminal history record to the FBI's Expungement Unit.

12. Does the FBI receive updated disposition information from the Office of Personnel Management's (OPM) NACI investigations? If yes, how many case files were provided by OPM over the last five years, and does the FBI update this information in its databases?

Response:

The FBI does not receive updated disposition information from the Office of Personnel Management.

13. Does the FBI receive updated disposition information from the Transportation Security Administration (TSA) for port worker and hazmat driver background checks? If yes, how many case files were provided by TSA over each of the past five years, and does the FBI update this information in its databases?

Response:

The FBI does not receive updated disposition information from the Transportation Security Administration.

Questions Posed by Senator Grassley

Fort Hood Shooting by Major Hasan

On February 3, 2011, the Homeland Security and Government Reform Committee (HSGAC) released a Committee Report that outlined lessons learned from the government's failure to prevent the Fort Hood attack by Major Nidal Hasan. The Committee reported that a "lead" came in to the FBI, but was not even assigned for 6 weeks. Then the investigator, waiting until the 90th day deadline arrived, did a superficial job on his report. To compound the problem, because this investigator was from the Department of Defense, even though he was on the joint terrorism task force, he was not provided full access to a key database that contained Hasan's communications, which likely

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.018

would have sparked a more in-depth inquiry. The report recommends that the FBI "*more convincingly* share information and coordinate operations with other federal, state, and local agencies."

14. Do all analysts, agents, and intelligence specialists who participate on Joint Terrorism Task Forces (JTTF) have access to FBI databases?

Response:

Yes, all Joint Terrorism Task Force (JTTF) participants have access to FBI databases once they complete required training and obtain the necessary security clearances.

Certain databases used by JTTF personnel are classified at the Top Secret/ Sensitive Compartmented Information level. Access to these systems is limited to those with an articulable need for access. The baseline suite of databases typically used by JTTF personnel, however, is classified at the Secret or Unclassified level and being assigned to a JTTF or counterterrorism matter is typically sufficient to obtain access to these databases.

The FBI's internal review after the Fort Hood attack identified a need to improve database training for JTTF members. To address this concern, the FBI initiated a surge in training to ensure that all on-board JTTF personnel – FBI employees and non-FBI task force officers, alike – received baseline training on and access to the databases identified as integral to JTTF investigations and operations. To accomplish this task, in January 2010 the FBI mandated that each field office send representatives to the FBI's training facility at Quantico, Virginia, to complete database training as part of a "train-the-trainer" program. Once trained, these individuals were tasked with training all of the JTTF members in their home divisions. By May 2010, when the surge was completed, 3,732 task force members had completed the training.

In order to ensure that new task force members receive timely and appropriate training going forward, the National Joint Terrorism Task Force has refined the JTTF orientation and training curriculum and developed a tracking mechanism to ensure that all JTTF members receive the training and access they need to use these databases effectively.

15. If so, why did the FBI limit the database access of the Defense Department Investigator in the case involving Major Hasan? If analysts, agents and intelligence specialists don't

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.019

have access to FBI/JTTF databases, then why are they on the task force?

Response:

As recognized in the report by the Senate Committee on Homeland Security and Governmental Affairs and as diagnosed shortly after the attack during the internal FBI review, the task force officer's lack of access to the FBI database at issue was not due to a policy of denying task force members such access. Rather, the lack of access was a training issue that has since been resolved, as described in response to Question 14, above. The task force officer in the case involving Major Hasan was unaware of a particular FBI database and thus did not seek or obtain access to it.

The FBI strives to provide each JTTF member with the training and tools necessary to perform the job. Each task force member, whether from the FBI or from a partner agency or department, must have the appropriate clearances and complete required training as a prerequisite to obtaining access to databases that contain sensitive information. Since the attack at Fort Hood, the FBI has taken steps to ensure that all task force members receive the training and access necessary to make efficient use of all available data sets.

16. Why would the FBI limit the database access of an individual serving on a JTTF?
Response:

Please see the responses to Questions 14 and 15, above.

Robert Kobus, FBI Whistleblower

Since I did not receive a response to my letter of March 31, I wanted to reiterate my questions about FBI whistleblower Robert Kobus. As you are aware, Kobus filed a claim of retaliation in November of 2005. In March of 2007, the Department of Justice (DOJ) Office of the Inspector General (OIG) found that the FBI had retaliated against Mr. Kobus for reporting time and attendance fraud by FBI agents.

It has been nearly six years since Mr. Kobus first filed his claim of retaliation, and four years since the DOJ OIG concluded that Mr. Kobus was retaliated against. This delay continues because the OIG's independent finding is subject to another layer of review at the DOJ Office of Attorney Recruitment and Management (OARM). This lengthy process has forced Mr. Kobus to rack up over $200,000 in legal fees. It is hard to understand how

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.020

whistleblowers can expect a resolution of their claims when the government can simply delay and delay until the whistleblower runs out of money.

Although you have frequently said that retaliation would not be tolerated, Mr. Kobus's former supervisor, Mary Galligan, was promoted to the position of Chief Inspector in June 2009. Attorney General Holder responded to written questions regarding Ms. Galligan's promotion in March 2010 and stated that a records search did not disclose any "pending" Inspector General investigations of Ms. Galligan at the time of her promotion. In fact, an investigation had already concluded - and the Inspector General found that her actions constituted retaliation. The FBI promoted her anyway. Then, the FBI promoted her again. In July 2010 she was named Special Agent in Charge (SAC) of Cyber/Special Operations for the FBI's New York Division.

17. Does the FBI believe whistleblowers should be protected against retaliation?

Response:

The FBI strongly supports protecting the rights of whistleblowers and recognizes the invaluable role that whistleblowers play in unearthing waste, fraud, and abuse.

18. Why did the FBI choose to promote Ms. Galligan despite the Inspector General's finding of whistleblower retaliation?

Response:

The FBI responded to this inquiry by letter to Senator Grassley dated 5/9/11. That letter is attached as an enclosure to these responses.

19. Was the FBI unaware of the Inspector General findings with regard to Ms. Galligan - as Attorney General Holder's written response implies? If so, please explain why and what steps the FBI took prior to her promotion to determine whether Ms. Galligan was the subject of findings of retaliation or other misconduct.

Response:

The FBI responded to this inquiry by letter to Senator Grassley dated 5/9/11. That letter is attached as an enclosure to these responses.

20. What has actually happened in the OARM process since the beginning of 2009? Please provide a detailed description of each procedural filing, response, or other action the FBI has taken in that process in the last two-and-a-half-years.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.021

Response:

The FBI responded to this inquiry by letter to Senator Grassley dated 5/9/11. That letter is attached as an enclosure to these responses.

21. Why has there been such an inordinate delay in reaching some finality in this case?

Response:

The FBI responded to this inquiry by letter to Senator Grassley dated 5/9/11. That letter is attached as an enclosure to these responses.

Communications Assistance for Law Enforcement

The Communications Assistance for Law Enforcement Act (CALEA) is legislation that requires electronic communications companies to provide information to law enforcement that is authorized by a court order. This law addresses the *capability* of electronic communication companies to provide the information, not the *authority* of law enforcement to obtain it. With the advancement of technology, the gap is widening between what the courts *authorize* agents to get and what companies are *capable* of providing.

22. Would the FBI agree that the Communications Assistance for Law Enforcement Act needs to be updated?

Response:

The Administration has convened an interagency working group to review the Going Dark problem and identify possible solutions. Any proposed legislation will be appropriately coordinated through the interagency process.

23. If Congress does not pass a law requiring compliance with this law, will this negatively affect the FBI's ability to collect what a judge has ordered them to get? Please provide any examples to support your position.

Response:

Please see the response to Question 22, above.

Maintaining Fiscal Responsibility Within the FBI

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.022

The FBI's budget request for FY 2012 is approximately $8.075 billion which represents an increase of $131 million over their FY 2011 budget request and also represents a four percent increase over their FY 2010 budget. The President has previously asked members of his own Cabinet to cut as much as $100 million from their respective budgets. Recently, the President asked federal agencies to make serious reductions within their information technology spending. Nevertheless, the FBI has requested approximately $10.495 million to support information technology (IT) needs though the FBI has assured members of the Senate that the FBI will not require additional funding to complete the Sentinel project, a virtual case management system with numerous financial issues.

In FY 2010, the FBI participated in a DOJ Southwest Border Supplemental request that augmented their FY 2010 budget by providing $16.7 million for 78 new positions, 44 of which were for special agents. The FBI's FY 2012 budget contains requests for increased spending in numerous areas such as "Operational Enablers", "Violent Crime in Indian Country" and the construction of a Central Records Complex (CRC). The FBI's budget request for "Operational Enablers" is approximately $2.4 million with acknowledgement that this amount is for "non-personnel". The FY 2012 budget also includes $9 million for an FBI presence in Indian Country. This amount includes 40 positions (24 agents) and $449,000 of the $9 million for "non-personnel".

Additionally, the FBI requests funding for the construction of a Central Records Complex (CRC) which will supposedly allow agents and analysts reliable access to pertinent intelligence and serve as a means of preserving administrative records. However, given the difficulties the FBI has encountered with the Sentinel project; it is questionable that agents or analysts could easily access records at the CRC for the foreseeable future.

24. Should the FBI be required to reduce its budget request, given that the FBI received an additional $16.7 million in a supplemental budget in FY2010 and the President supports federal agencies cutting their spending by as much as 5%?

Response:

The FBI understands the need to reduce federal spending and has proposed $70 million in reductions in our FY 2012 Request to Congress.

25. Does the FBI believe there are any programs or areas available for reduction within your budget request?

Response:

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.023

The FBI's FY 2012 Request to Congress includes a $26 million reduction in the Secure Work Environment program, a $6 million reduction in the relocation program, a $6 million reduction in Network and Intrusion Analysis activities, and nearly $16 million in reductions related to office space, facilities, task forces, information technology, and administrative costs.

26. The Central Records Complex will allegedly allow agents and analysts reliable access to pertinent intelligence. However, given that your virtual case management system, the Sentinel project, has so many problems isn't it unlikely that agents or analysts could easily access records at the CRC for the foreseeable future?

Response:

The Central Records Complex (CRC) will immediately speed access to the FBI's paper records through efficiencies in physical management. Instead of retrieving paper files from over 400 locations worldwide, locating these files centrally in the CRC will permit expedited, centralized access to the information contained in billions of pages of documents. Because many paper files may never be requested, it would not be an efficient use of FBI resources to digitize all 178 linear miles of existing paper files. The FBI is, though, currently scanning any paper files retrieved from our archives for investigative purposes.

The CRC approach to physical records management and on-demand scanning is independent of the Sentinel deployment schedule. The FBI's Records Management Division is, though, working closely with the Sentinel team to develop the electronic record solution in the new case management system. While the CRC file request and access protocol will initially operate outside of Sentinel, the process is being designed to link to Sentinel once the new case management system is operational.

27. How does the FBI justify the request to construct the Central Records Complex (CRC)?

Response:

As noted above, official FBI investigative records are currently found in more than 400 locations worldwide. Because the FBI's ability to successfully prevent a developing terrorist plot may depend on the speed with which we can access information, prompt access to all of our records is essential. Centralizing these

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.024

records at the Central Records Complex (CRC) will ensure that agents and analysts can access these records electronically within 1 hour of demand. Centralized location in the CRC will also help ensure vital information can be quickly shared with our partners in the Intelligence and Law Enforcement communities.

28. Many American Indian tribal communities have endured significant economic hardships, why should Congress provide the FBI more money for a presence in Indian Country when that funding, which is approximately $9 million, could be given directly to tribal law enforcement?

Response:

The FBI is responsible for investigating all felonies within the approximately 200 Indian Reservations throughout the United States. These felonies include murder, child sexual and physical assaults, other violent assaults, and drug offenses, with significant criminal activity involving gangs. Because most Tribal law enforcement authorities do not exercise jurisdiction to investigate felonies, any directly allocated funding would be used to investigate misdemeanor violations. Omitting FBI involvement from Tribal law enforcement efforts would also deprive those communities of access to the expertise, technology, and other resources that are often necessary to successfully prepare a case for federal prosecution.

FBI Resources for Fighting Health Care

Last December, I sent a letter to DOJ and HHS requesting information about their efforts to combat health care fraud. Part of my request was for a detailed breakdown of HCFAC funding allocated to the FBI. The response I received in January did not address my specific requests and provided little more than the vague information already included in the annual HCFAC report. The President's FY 2012 budget requests an increase of $63.4 million for DOJ to combat health care fraud. I agree that stopping criminals from stealing precious resources must be a priority. I have introduced legislation that would help the federal government in these efforts. However, if Congress is to increase funding for this goal, we need to know how that money is being spent.

29. The administration has publicly stated that fighting health care fraud is one of its top priorities. How does the FBI play a significant role in executing this priority? Please explain how the FBI contributes to combating health care fraud.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.025

Response:

The FBI is in the unique position of having investigative authority with respect to both the federal and private health insurance programs. The FBI leverages the resources it dedicates to both areas through investigative partnerships with other federal agencies, including the U.S. Department of Health and Human Services Office of Inspector General (HHS/OIG), the Drug Enforcement Administration (DEA), the U.S. Food and Drug Administration, the Defense Criminal Investigative Service, the Office of Personnel Management (OPM), and the IRS, as well as with various state and local agencies. The FBI also works extensively with such national groups as the National Health Care Anti-Fraud Association, the National Insurance Crime Bureau, and the Blue Cross and Blue Shield Association to expose and investigate fraud within the system.

FBI investigators work through coordinated initiatives, task forces, and undercover operations to identify and pursue the most egregious perpetrators of health care fraud, often finding organized criminal activity in the operation of medical clinics, independent diagnostic testing facilities, durable medical equipment companies, and other health care facilities. Task force operations often include active participation by the relevant United States Attorney's Office (USAO), the Criminal Investigative arm of the IRS, HHS/OIG, the state prosecutor or state Attorney General's office, state health care fraud investigative agencies, and local law enforcement personnel. For example, the FBI currently supports the Health Care Fraud Prevention and Enforcement Action Medicare Strike Force operations in Miami, New York City, Houston, Tampa, Detroit, Los Angeles, Baton Rouge, Chicago, and Dallas. In FY 2010, Strike Force accomplishments included 140 indictments involving charges against 284 defendants who collectively billed the Medicare program for more than $590 million. Those charges led to 217 guilty pleas and 19 jury trials that resulted in guilty verdicts against 23 defendants.

In addition, in FY 2010 the FBI expanded its involvement in *qui tam* investigations involving major pharmaceutical manufacturers, including the $2.3 billion Pfizer criminal/civil settlement, the $126 million Omnicare civil settlement, and the $600 million Allergan criminal/civil settlement. The activities investigated included kickbacks, off-label marketing, misbranding, and the submission of fraudulent/false claims to Medicare and Medicaid.

In FY 2010, more than 400 FBI health care fraud investigators and analysts received training and the FBI conducted a wide range of training for external

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.026

audiences involved in the investigation of health care fraud matters. The FBI has teamed with the Department of Justice (DOJ), the United States Attorneys, and HHS/OIG to expand both the content and the recipients of training related to health care fraud investigations. The expanded training curriculum will address sophisticated and advanced investigative techniques and will include the roles of traditional organized crime and extraterritorial groups in health care fraud schemes. Joint training will include sessions regarding common health care fraud activities, identity theft, money laundering, and criminal enterprise targeting.

30. Please provide a detailed analysis of how mandatory HCFAC funding is allocated at the FBI?

Response:

In FY 2011 the FBI was allocated $126.2 million in dedicated mandatory funding for health care fraud enforcement by the Health Insurance Portability and Accountability Act plus a $2.1 million inflation adjustment provided by the Affordable Care Act. Another $5.6 million of prior-year funding is available in 2011 in discretionary Health Care Fraud and Abuse Control program funds, for a total projected funding level of $133.9 million in FY 2011. This funding is used to support 769 positions (460 Special Agent and 309 professional support positions). Of this $133.9 million, $106.5 million will fund personnel compensation and benefits. The remaining $27.4 million will be used for space and utilities, operational support services (including the assistance of experts), supplies and equipment, travel and transportation, case funds, and printing and reproduction.

Questions Posed by Senator Hatch

Iraq Detainees

As the deadline for the withdrawal of United States armed forces from Iraq approaches, there are approximately 200 detainees in U.S. custody in Iraq. Please provide the following information regarding FBI activities with respect to enemy combatants captured in Iraq:

31. Has the FBI participated in or conducted threat assessments of foreign nationals currently detained in Iraq to assess the likelihood of these individuals returning to hostilities against United States citizens in the event they are turned over to Iraqi custody and released?

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.027

Response:

The FBI has not conducted assessments of the detainees with the specific purpose of ascertaining whether they will return to hostilities against U.S. citizens. Generally, the FBI interviews detainees only if there is a possible investigative nexus to known subjects or incidents in which the FBI has an interest. The FBI does, though, provide any information in our possession to DoD, which assesses the threat posed by these detainees.

32. How many detainees captured on the battlefield were interviewed by FBI personnel?

Response:

FBI records indicate that 48 of the current 204 detainees at Camp Cropper were interviewed by FBI personnel.

33. Were Miranda rights read to any of the Iraq battlefield detainees during interviews?

Response:

Miranda warnings are never given on the battlefield or in any other circumstance in which they could have an adverse impact on military or intelligence operations.

In rare circumstances in Iraq, the FBI provided Miranda warnings to certain detainees, but only after consultation with DOJ and other agencies and never if a determination was made that the warnings would hinder our counterterrorism efforts.

34. Has the FBI conducted any assessments or investigations to determine if any of the individuals currently in custody could be the subject of a criminal investigation for their actions against U.S. citizens to include but not limited to the crime of kidnapping and murder of United States citizens?

Response:

In 2007, DOJ and the Multi-National Forces - Iraq formed the Law and Order Task Force (LAOTF), a joint Iraqi, civilian, and military capacity building organization that has focused on building Iraqi capacity for independent, evidence-based, transparent, and even-handed investigation and trial of major crimes before the Central Criminal Court of Iraq. The LAOTF has been the lead

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.028

organization developing prosecution packages involving the detainees. Along with the DoD Intelligence Directorate (J2) and the Iraqi Ministry of the Interior, the LAOTF has been working to develop prosecution packages that can assist the Government of Iraq (GoI) in conducting Iraqi prosecutions. The LAOTF and DoD have examined detainee case files to identify information of evidentiary value, and are reviewing classified evidence that may assist Iraqi prosecutions with a view toward declassification and release.

FBI investigations of detainees are not designated as criminal or non-criminal, but are national security investigations that are part of the FBI's counterterrorism mission. The information collected by the FBI during the investigation of detainees in Iraq may support its role within the intelligence community as well as potential criminal charges against the detainee. The FBI is not responsible for determining whether charges are warranted or in what forum charges might be brought. Within that framework, the FBI has investigated numerous individuals currently in custody based on statements they have made regarding either their own actions or the actions of others.

Ali Mussa Daqduq

In March 2007, Ali Musa Daqduq, a Lebanese national with a significant association to Hezbollah and Iranian Special Forces, was captured in Iraq. He was captured with Qais al Khazali and Laith al Khazali.

In January 2007, Daqduq and the Khazali brothers planned and coordinated an attack and botched kidnapping attempt on U.S. forces in Karbala that left 5 United States soldiers dead and 3 others wounded. The trio was captured near Basra on March 20, 2007.

Ultimately, despite an executive order prohibiting the United States from negotiating with terrorists, Laith and Qais al Khazali were released in exchange for a British national that had been kidnapped by Qais al Khazali's League of Righteousness confederates. However, Hezbollah operative Ali Musa Daqduq, remains in United States custody and is detained in Iraq.

35. Has the FBI initiated a criminal investigation into the actions of Daqduq and his role in the death of U.S. soldiers in January 2007?

Response:

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

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.029

36. Has the FBI consulted with the Department of Justice and the Department of Defense to determine if Daqduq's actions constituted a crime of war or a violation of federal law (e.g. 18 USC 1114)?

Response:

The FBI is not responsible for determining what, if any, charges might be appropriate for a particular detainee, or in what forum to bring those charges. DOJ and the Office of Military Commissions are aware of the FBI's investigation of Daqduq and the information developed by the FBI.

37. What determinations has the FBI made with respect to pursuing a criminal investigation of Ali Musa Daqduq?

Response:

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

FBI Criminal Investigations

In FY2000, the FBI had 682 field agents investigating organized crime and 433 cases were opened. In FY 2004, the FBI had 433 field agents investigating organized crime and only 263 cases were opened. According to the Department of Justice Inspector General, the FBI only utilized 443 for organized crime investigations. The FBI also disclosed to the Inspector General that they did in fact underutilize agents for organized crime investigations. Audits by the Inspector General confirmed that the FBI had in fact transferred agents from traditional crime squads to squads with a counter-terrorism mission. In fact, Director Mueller, you have testified previously that resources have shifted away from traditional crime fighting so that the FBI could focus on terror investigations.

There are other federal criminal investigative agencies that could easily step in and continue on with traditional crime investigations. For example, illicit drug trafficking is investigated by the DEA. Human trafficking and child pornography is investigated by ICE. Mortgage fraud, cyber and certain white collar crimes are investigated by the Secret Service. Fugitive investigations can be carried on by the Marshal Service.

38. With so much of the FBI's attention and focus directed at foreign counter-intelligence and terrorism investigations, should the FBI relinquish some of its traditional crime investigations?

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.030

Response:

Since the attacks of 2001, the FBI has transformed itself into a threat-focused, intelligence-led national security agency whose highest priority is to protect our nation from terrorist attack. Terrorism is, though, by no means our only priority. We have expanded our ability to confront the increased threat of cyber-based attacks and we continue our efforts to combat public corruption, transnational organized crime, major white-collar crime, and significant violent crimes.

In the wake of the September 11th attacks, the FBI moved 2,000 agents from the criminal program (1,500 from the drug program and another 500 from smaller white-collar criminal cases) to the national security program. At the time, the FBI coordinated with DEA to ensure continuity in the drug enforcement program and also worked with state and local law enforcement authorities to develop programs to address lower-level white-collar crime. Today's FBI is evenly distributed between Criminal and Counterterrorism programs. In the FBI's Criminal program, we have roughly 50,000 cases ongoing at any given time. We work closely with our partners and focus on those areas where we can contribute the most "value added."

The FBI recognizes that fighting public corruption is vital to preserving our democracy, protecting our borders, and securing our communities. For this reason, public corruption remains our top criminal priority. On 10/10/10, 89 law enforcement officers and 44 others were arrested and charged in Puerto Rico as part of Operation Guard Shack, the largest police corruption investigation in the history of the FBI. Nearly 750 FBI agents were flown in to Puerto Rico from across the U.S. to assist in these arrests. This two-year, multi-jurisdictional, multi-agency operation sent a powerful message - that corruption among our public officials will not be tolerated.

Although the FBI has been forced to reduce the number of agents working government fraud matters since 9/11/01, we continue to address serious fraud involving federal funds, as exemplified by the FBI's current priority initiatives to address fraud relating to economic stimulus funding and contract-related fraud in Iraq, Afghanistan, and Kuwait. In partnership with DOJ's Antitrust Division, the FBI has also devoted substantial resources to the investigation of significant antitrust matters involving national and international price fixing, bid rigging, and market allocation conspiracies. Over the past 5 years, these investigations have resulted in 130 convictions, $61.2 million in restitution, and $2.8 billion in fines.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.031

The FBI is also concerned with the increased presence and impact of international organized criminal enterprises. While some believe that organized crime is a thing of the past, unfortunately this is not the case. Traditional criminal syndicates still con, extort, and intimidate American citizens. In recent years, we have seen a shift from regional families with clear structures to flat, fluid networks with global reach. These international enterprises are running multi-national, multi-billion-dollar schemes. Pursuant to a 10/13/10 health care fraud takedown, 73 members and associates of organized crime groups (including, for example, the Mirzoyan-Terdjanian Organization) were among those indicted for more than $163 million in health care fraud offenses. Among these defendants is Armen Kazarian, who is alleged to be a "vory-v-zakone," a term that is translated as "thief-in-law" and refers to a member of a select group of high-level criminals from the countries that previously comprised the former Soviet Union, including Armenia.

Over the past year, the FBI has continued to uncover massive financial frauds that have devastated communities and threatened our economy. At the end of FY 2010, for example, the FBI was engaged in over 2,300 active corporate and securities fraud investigations and had contributed to over 600 indictments and more than 500 convictions. During the same time frame, the FBI was involved in over 3,000 ongoing mortgage fraud investigations and had participated in over 1,500 indictments and nearly 1,000 convictions. Nearly 70 percent of those investigations involved losses of more than $1 million each.

In June 2003, the FBI, DOJ's Child Exploitation and Obscenity Section, and the National Center for Missing and Exploited Children joined forces to launch the Innocence Lost National Initiative (ILNI), targeting the growing problem of domestic sex trafficking of children in the United States. Each of the ILNI's 41 task forces and working groups throughout the United States include federal, state, and local law enforcement agencies working in tandem with USAOs. The FBI's Crimes Against Children Unit also coordinates an ongoing national sting operation entitled Operation Cross Country to combat domestic sex trafficking of children. Through Operation Cross Country, more than 2,100 law enforcement officers have joined together to rescue child victims and to apprehend those who victimize them. As a result, 248 child victims have been safely recovered and we have arrested 322 pimps engaged in the commercial sexual exploitation of children.

The FBI has maintained its longstanding focus on traditional organized crime,

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.032

arresting 127 associates of La Cosa Nostra in January 2011 for a wide range of illegal activities (including murder, arson, narcotics trafficking, extortion, robbery, illegal gambling, labor racketeering, and loan sharking). In addition, the FBI continues to investigate street gang members through its Violent Gang Safe Streets Task Forces. This program leverages federal, state, and local law enforcement resources to investigate violent gangs in urban and suburban communities. There are currently 231 Safe Streets Task Forces, comprised of 1,055 FBI Special Agents and 2,251 other federal, state, and local officers.

With clear focus on the importance of avoiding the duplication of functions either within the FBI or with our partners, the FBI has successfully maximized its resources and relationships with its law enforcement partners, domestically and internationally, to address its priority criminal investigative responsibilities. Despite its shift in priorities, the FBI's traditional criminal investigations remain a vital part of the FBI and a tremendous source of actionable intelligence.

39. Would the FBI be in a position to better protect the American public from future terror attacks if it focused solely on terror investigations?

Response:

The FBI has a broad mission with varied and competing challenges. In order to discipline the FBI's approach to these challenges, we have considered the interaction of three factors: (1) the significance of the threat to the security of the United States as expressed by the President in National Security Presidential Decision Directive 26; (2) the priority the American public places on various threats; and (3) the degree to which addressing the threat falls most exclusively within the FBI's jurisdiction. Weighing and evaluating these factors resulted in the FBI's top ten priorities. (The first eight are listed in order of priority. The final points (collaborative partnerships and technology improvement) are key enabling functions that are of such importance they merit inclusion.) The priorities are:

1. Protect the United States from terrorist attack;
2. Protect the United States against foreign intelligence operations and espionage;
3. Protect the United States against cyber-based attacks and high-technology crimes;
4. Combat public corruption at all levels;
5. Protect civil rights;
6. Combat transnational and national criminal organizations and enterprises;

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.033

7. Combat major white collar crime;
8. Combat significant violent crime;
9. Support federal, state, local, and international partners;
10. Upgrade technology to successfully perform the FBI's mission.

The FBI staffs and works high priority matters before lower ones, with resources being allocated and applied to each FBI mission according to its priority. The counterterrorism effort has received significant financial and human capital resources since 9/11/01; those resources have been used to build our capabilities and to re-engineer the FBI into a proactive, intelligence-gathering organization committed to protecting the United States from future terrorist attacks.

While our national security efforts remain our top priority, the FBI continues to fulfill our crime-fighting responsibilities as well, focusing on public corruption as the top criminal priority for the FBI. Please see the response to Question 38, above, regarding the FBI's continued commitment to addressing traditional criminal matters.

40. Based on the number of personnel assigned to traditional criminal investigations and the significant reduction of cases and prosecutions generated post 9/11, how can the FBI defend or justify its current Staffing levels when it has clearly shifted investigative priorities to terror investigations?

Response:

Please see the response to Question 38, above.

Indian Country Investigations

According to the Government Accountability Office, for fiscal years 2005 through 2009, the FBI referred 5, 500 cases to offices of the United States Attorney's Office. That accounted for roughly 55% of all the cases referred for prosecution (violent and non-violent crimes). The United States Attorney's Offices declined 46% of FBI cases for prosecution. Considering that assault and sexual abuse crimes were the leading offense for Indian Country investigations it is troubling that more than half of these cases are declined.

41. Is there a "disconnect" between the USAO and the FBI with respect to Indian Country investigations?

Response:

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.034

The FBI and USAOs communicate well and work well together with respect to both Indian Country investigations and other matters. The FBI investigates myriad Indian Country violations and FBI agents work closely and effectively with Assistant United States Attorneys (AUSAs) throughout the investigative process to ensure successful prosecutions whenever possible. Cases referred by the FBI for prosecution may be declined by USAOs for a variety of reasons, including insufficient evidence of criminal intent, uncooperative witnesses, and events that fall completely outside the control of either the FBI or the USAO.

42. Do you believe that prosecutorial guidelines and investigative guidelines are out of sync?

Response:

The FBI has no reason to believe that prosecutorial guidelines and investigative guidelines are out of sync. The FBI investigates felony violations occurring in Indian Country and works with the cognizant USAO to determine the prosecutorial merits of each case.

43. What can the FBI do to reduce the number of declinations for offenses committed on Indian Country?

Response:

While the FBI works closely with the USAO throughout the investigative stage, the determination of whether it is appropriate to move forward with prosecution ultimately lies within the discretion of the USAO.

FBI agents routinely involve AUSAs at all stages of investigation. This ongoing collaboration helps ensure that pending investigations satisfy the legal requirements for successful prosecution. Declination by the USAO does not necessarily mean the subject will not be held accountable - the FBI's investigation may support successful prosecution in another jurisdiction (state, local, or tribal).

Questions Posed by Senator Kyl

44. It has been reported that the sixth largest cellular provider, U.S. Cellular, is contemplating having Huawei build out its new 4G network.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.035

a. Considering how concerned the U.S. government was about potential agreements between Huawei and AT&T and Huawei and Sprint – so concerned that it intervened with the companies – what would your concerns be about such a contract?

Response:

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

b. For national security purposes, should we expand the ability of groups like Team Telecom to review significant purchases of telecommunications equipment that will be integrated into U.S. infrastructure? Should there be a reporting mechanism for such purchases?

Response:

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

45. As you know, companies like Huawei and ZTE Corporation have close links to the People's Liberation Army and receive Chinese government support of such magnitude that it suggests these companies may act as foreign agents for the Chinese government.

a. Do you have a policy concerning FBI systems and use of equipment from these two companies?

Response:

As required by Director of Central Intelligence Directive 7/6, "Community Acquisition Risk Center" (March 2005), the FBI established policies and procedures for the screening of vendors in the government's supply chain that may involve foreign ownership, control, or influence or association with foreign intelligence services, terrorist organizations, or criminal enterprises. Any procurement that involves services requiring access to classified information or the procurement of critical assets (defined as information technology hardware or software associated with an FBI Federal Information Security Management Act system or audio-visual or telecommunications equipment) is required to undergo a company threat assessment (CTA). No FBI procurements involving Huawei or ZTE Corporation have been initiated since the establishment of the FBI's CTA program in October 2005.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.036

b. Would you feel comfortable with Huawei becoming integrated into the FBI supply chain?

Response:

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

46. According to the FBI's Cyber Crime division website, the FBI "lead[s] the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds." With that role in mind, I understand that Huawei is making significant in-roads into the U.S. market by providing equipment to counties and local governments throughout the United States, and also by using companies like SYNNEX and Force10 Networks to resell their products in the United States. Is the FBI – and, to your knowledge, the U.S. government – reviewing Huawei sales at the local level and through other vendors for national security concerns?

Response:

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

47. We understand that Huawei has partnered with the company Hibernia to help build and deploy a cable between New York and the UK that will transmit sensitive data including market information from the New York Stock Exchange. What is the group called "Team Telecom" doing to review Huawei's partnership with Hibernia and the cable license involved with this cable landing? Should a PLA-linked firm be building a fiber optic line that is supposed to be "ultra secure"?

Response:

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

48. Although the Committee on Foreign Investment in the United States (CFIUS) was successful in addressing national and cyber security matters in Huawei's attempted acquisition of the assets of the California company 3-Leaf, this transaction also showed that CFIUS is a limited tool. How can Congress provide the U.S. government with the right tools to deal with deficiencies in CFIUS' ability to address national security matters beyond just acquisitions?

Response:

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.037

The FBI defers to the Department of the Treasury regarding the appropriate scope of the Committee on Foreign Investment in the United States (CFIUS). We would be pleased to work with the Department of Treasury, as Chair of CFIUS, and others in DOJ to identify legislative or regulatory measures that may enhance CFIUS' ability to protect national security.

Questions Posed by Senator Sessions

49. During the March 30, 2011 hearing, both Senator Graham and I asked, in the context of other questions, about your view on whether *Miranda* warnings can be counterproductive to intelligence gathering if given, as required, at the outset of a custodial interrogation by law enforcement. You were unable to give a full answer due to other matters being raised at the same time, and your response is unclear from the unofficial transcript.

a. To give you the opportunity to complete your answer, please state your view on whether *Miranda* warnings can be counterproductive to intelligence gathering if given, as required, at the outset of a custodial interrogation by law enforcement.

b. Aside from Umar Farouk Abdulmutallab, who reportedly invoked his right to remain silent for some period of time after being given *Miranda* warnings, have other terror suspects during your tenure as Director invoked silence, stopped cooperating, or delayed their cooperation for some period of time after receiving *Miranda* warnings?

Response to subparts a and b:

While there is no Constitutional requirement that *Miranda* warnings be given "at the outset of a custodial interrogation by law enforcement," the Constitution does generally require such warnings to have been given if the statements taken during custodial interrogation are to be admitted in an Article III court against the arrestee during the government's case in chief. Even then, *New York v. Quarles*, 467 U.S. 649 (1984), makes clear that the fruits of interrogation reasonably prompted by an immediate concern for the safety of the public or the arresting agents will be admissible, notwithstanding the absence of *Miranda* warnings.

Some terrorism suspects arrested in the United States have invoked their right to remain silent after being provided *Miranda* warnings, while others have not. Obtaining actionable intelligence is the FBI's highest priority. The FBI's longstanding approach to obtaining actionable intelligence from a terrorist or a

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.038

criminal is to use rapport building techniques during questioning. Generally that approach is effective. When it is not, and the subject is being held in connection with a criminal proceeding, the FBI will work with the USAO to attempt to persuade the defendant to cooperate, using the leverage that comes with a criminal prosecution to facilitate that discussion.

50. If a foreign terrorist who is a member of al Qaeda is detained as an unprivileged enemy combatant and placed in military custody for intelligence-gathering interrogation, are *Miranda* warnings required?

Response:

DoD is best able to address the protocol it follows when it interrogates unprivileged enemy combatants captured outside the United States.

In recent history, only two individuals have been arrested in the United States and then subsequently placed into military custody as enemy combatants: Jose Padilla and Ali Al Marri. In both instances, the decision to declare the person an enemy combatant and to transfer him to military custody was made by the President well after the initial detention and well after the person had been provided *Miranda* warnings. In both cases, the transfer to military custody raised serious statutory and constitutional questions in the courts. Both men were later returned to the civilian criminal justice system and convicted.

51. In your testimony at the March 30, 2011 hearing, you mentioned the obligation to bring a terror suspect before a magistrate within 24 to 48 hours.

a. The obligation you mention is a constitutionally-based one that applies to criminal detention, correct?

Response:

The requirement to present an arrestee to a magistrate comes principally from the Federal Rules of Criminal Procedure. Rule 5(a), which has the force of law, requires that "a person making an arrest within the United States must take a defendant without unnecessary delay before a magistrate judge." While the facts and circumstances of a case govern what constitutes a reasonable time for presentment to a magistrate judge for the purposes of Rule 5, the Supreme Court has indicated that delay for the purpose of interrogation is the "epitome" of unnecessary delay. The Due Process Clause of the Fifth Amendment to the U.S.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.039

Constitution may also impose limits on delays in presentment that "shock the conscience." Like *Miranda* rights, the presentment requirement can be waived if the defendant does so knowingly and voluntarily.

Separate and distinct from the presentment requirement of Rule 5, the courts have determined that the Fourth Amendment requires a "prompt" judicial determination of probable cause after a warrantless arrest. The arrestee need not be present for this determination (although it can occur simultaneously with presentment). The Supreme Court has determined that the "promptness" requirement will generally be satisfied if the judicial determination of probable cause is made within 48 hours of arrest.

b. Do you agree that there is no similar obligation to bring a terror suspect, specifically a foreign member of al Qaeda, before a magistrate within 24 to 48 hours if the al Qaeda member is being held in military custody as an unprivileged enemy belligerent?

Response:

Please see the response to Question 50, above.

52. In your previous responses to questions for the record following the July 2010 oversight hearing, you mentioned two recent cases where individuals were detained in the United States and thereafter transferred to military custody. Were the Nazi saboteurs at issue in *Ex Parte Quirin* detained by the FBI before being transferred to military custody for military commission trial?

Response:

As described in *Ex Parte Quirin*, 317 U.S. 1 (1942), the Nazi saboteurs were initially taken into custody by FBI agents. Approximately one week after the last saboteur had been taken into FBI custody, the President appointed a Military Commission and directed that it try the saboteurs. At the direction of the Attorney General, the FBI then surrendered custody to the Provost Marshal of the Military District of Washington. The Secretary of War directed the Provost Marshal to receive and keep the saboteurs in custody for trial before the Military Commission.

The FBI advised at least one of the saboteurs (Ernest Burger) of his right to be arraigned by a duly authorized judicial officer or magistrate. The arrestee waived that right and consented to remain in the FBI's custody. We have been unable to

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.040

locate records indicating whether civilian charges were brought against any of the saboteurs prior to the President's order to transfer custody to the Provost Marshal. Nevertheless, as with the more recent examples of enemy combatants arrested in the United States, it appears that the decision to transfer the Nazi saboteurs from civilian to military custody was made by the President.

53. In response 40.d. to the questions for the record submitted following your July 2010 appearance before the Committee, you answered a question about whether "the administration [has] created some sort of emergency inter-agency process to make status determinations in terrorism cases – to determine, for example, whether a foreign al Qaeda agent should be held as a criminal defendant or in military custody as an enemy belligerent" by noting that there is "extensive interagency cooperation and coordination" and "prompt notification of other agencies." You did not state whether the administration has created an interagency process for status determinations in the aftermath of a terrorism arrest or detention in the United States.

a. Has the administration created or articulated a defined process to make such decisions?

Response:

The FBI is not in a decision-making role regarding status determinations for operational terrorism suspects arrested in the United States. The FBI notifies other agencies when it intends to arrest an operational terrorism subject in the United States. Notification informs these agencies that the suspect will be handled in accordance with the requirements of the criminal justice system and it allows them to propose any alternatives they believe might be appropriate.

b. Is that process set forth in writing? If so, would you please provide it to the Committee, including as a classified submission if necessary.

Response:

Please see the response to subpart a, above.

54. In response 40.g. to the questions for the record submitted following your July 2010 oversight testimony, you revealed that Nigerian Embassy officials had access to Umar Farouk Abdulmutallab within one day of his arrest.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.041

a. Your answer suggests that consular notification was unnecessary in this case because the Nigerian Embassy officials contacted the FBI on their own upon learning of Mr. Abdulmutallab's arrest via media reports. Is this correct?

Response:

Nigeria is among the countries for which consular notification is mandatory when their citizens are arrested or detained in the United States. In this particular case, the issue of consular notification was made moot by the fact that Nigerian Embassy officials learned of the arrest and sought access prior to formal notification by the FBI. As indicated in the response to the July 2010 Question for the Record referenced above, U.S. Customs and Border Protection officers detained Abdulmutallab at the airport on December 25, 2009. Although no consular notification was attempted on that date, officials from the Nigerian Embassy appeared the following day at the FBI's Detroit office, having been alerted by the news media that Abdulmutallab was a Nigerian national and was in custody. Embassy officials were granted access to Abdulmutallab the same day. The USAO was aware of the Nigerian Embassy's involvement and did not separately notify the consulate.

b. Is there an established policy for consular notification, including time guidelines for such notification, which will apply to future terrorism arrests? If so, is that policy in writing and will you provide it to the Committee, including as a classified submission if necessary?

Response:

28 C.F.R. § 50.5, *Notification of Consular Officers upon the arrest of foreign national,* establishes DOJ's procedures for consular notification. Section 50.5(a) provides as follows.

> (1) In every case in which a foreign national is arrested the arresting officer shall inform the foreign national that his consul will be advised of his arrest unless he does not wish such notification to be given. If the foreign national does not wish to have his consul notified, the arresting officer shall also inform him that in the event there is a treaty in force between the United States and his country which requires such notification, his consul must be

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.042

notified regardless of his wishes and, if such is the case, he will be advised of such notification by the U.S. Attorney.

(2) In all cases (including those where the foreign national has stated that he does not wish his consul to be notified) the local office of the Federal Bureau of Investigation or the local Marshal's office, as the case may be, shall inform the nearest U.S. Attorney of the arrest and of the arrested person's wishes regarding consular notification.

In addition, the U.S. Department of State maintains a Consular Notification and Access Manual, which provides comprehensive guidance on compliance with U.S. consular notification and access obligations. That manual is posted on the Department of State website at www.travel.state.gov/consularnotification.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.043

ENCLOSURE

QUESTIONS 18, 19, 20, AND 21

5/9/11 LETTER FROM THE FBI'S OFFICE OF CONGRESSIONAL AFFAIRS TO SENATOR GRASSLEY

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.044

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

May 9, 2011

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Grassley:

This is in response to your letter dated March 31, 2011, seeking information concerning a claim of retaliation filed by Mr. Robert Kobus. Responses to your specific questions are set forth below.

1. **Why did the FBI choose to promote Ms. Galligan despite the Inspector General's finding of whistleblower retaliation?**

Prior to any executive promotion or selection within the FBI, the FBI reviews the disciplinary records of the FBI's Office of Professional Responsibility (OPR), Inspection Division, Office of Equal Employment Opportunity Affairs, and Security Division, as well as the records of DOJ's Office of the Inspector General (OIG), OPR, and Criminal Division, for all prospective candidates.

Internal disciplinary reviews, covering Mary Galligan's entire career, were conducted prior to her selection as Chief Inspector. DOJ records did not disclose any pending OIG investigation regarding Ms. Galligan, and the FBI's OPR records revealed that an allegation that Ms. Galligan had retaliated against an FBI employee was unsubstantiated.

Following these checks, on June 29, 2009, Ms. Galligan was selected for the position of Chief Inspector because she was assessed to be the best qualified for the position.

2. **Was the FBI unaware of the Inspector General findings with regard to Ms. Galligan - as Attorney General Holder's written response implies? If so, please explain why and what steps the FBI took prior to her promotion to determine whether Ms. Galligan was the subject of findings of retaliation or other misconduct.**

The OIG reviewed the claim that a number of different personnel actions involving Mr. Kobus were retaliatory. The complained-of decisions were made by a number of different executives and the OIG concluded, as to some of the decisions, that there were "reasonable grounds to believe that Kobus' protected disclosure was a contributing factor." That finding was submitted to the FBI's OPR for adjudication; as to Ms. Galligan, OPR concluded that the allegation of retaliation was unsubstantiated. While the FBI was aware of the OIG finding, the information considered in connection with Ms. Galligan's promotion was limited to the outcome of the OPR review and other records checks as described above. This is standard procedure for SES promotions. It is intended to be consistent with the procedures we are required, by virtue of a court-ordered settlement decree, to use when considering discipline as part of the making mid-level promotion process.

3. What has actually happened in the OARM process since the beginning of 2009? Please provide a detailed description of each procedural filing, response, or other action the FBI has taken in that process in the last two-and-a-half-years.

Applicable regulations require that, when the office that conducts the investigation into a complainant's reprisal claims finds reasonable grounds to believe that there has been reprisal, that "conducting office" must report this conclusion to DOJ's Office of Attorney Recruitment and Management (OARM) (28 C.F.R. § 27.4(a)). OARM conducts a de novo review of the matter and, if it determines that it has jurisdiction to adjudicate the matter, the parties engage in discovery and proceed to arguments on the merits of complainant's reprisal claims. The complainant bears the burden of proving by preponderant evidence that he exhausted his claims and that he made a protected disclosure that was a contributing factor in the FBI's decision to take or fail to take (or threaten to take or fail to take) a personnel action against him. (28 C.F.R. § 27.4(e)(1)). If complainant meets that burden of proof, OARM will order corrective action as authorized by 28 C.F.R. § 27.4(f), unless the FBI proves by clear and convincing evidence that it would have taken the same personnel action against complainant in absence of his disclosure. (28 C.F.R. § 27.4(e)(1); (2)).

The FBI has responded as required during the proceedings before OARM. From December 2008 through approximately April 23, 2009, the FBI and Mr. Kobus prepared and filed their respective briefs on the merits of Mr. Kobus' claim. Mr. Kobus filed his post-discovery brief on the merits of his Request for Corrective Action on December 19, 2008; the FBI filed its brief on the merits on February 13, 2009; and, on March 6, 2009, Complainant replied to the FBI's brief. The FBI filed a surreply on April 1, 2009, and Mr. Kobus filed a limited response thereto on April 23, 2009. On October 19, 2009, both Mr. Kobus and the FBI participated in a discovery hearing with OARM involving one outstanding evidentiary item.

The matter is pending before the Director of OARM. OARM may make a merits determination based solely on the written record, or after affording the parties a full administrative hearing (to include witnesses' testimonies and the parties presentation of additional evidence and/or arguments). 28 C.F.R. § 27.4(e)(3).

71557.046

4. **Why has there been such an inordinate delay in reaching some finality in this case?**

The FBI recommends that questions regarding the process employed by OARM be directed to that office.

The FBI strongly supports protecting the rights of whistleblowers and recognizes the invaluable role that whistleblowers play in unearthing waste, fraud, and abuse. We appreciate your interest in this issue and your continued support for the FBI's mission.

Sincerely,

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

SUBMISSIONS FOR THE RECORD

STATEMENT OF SENATOR PATRICK LEAHY (D-VT.),
CHAIRMAN, SENATE JUDICIARY COMMITTEE
HEARING ON OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION
MARCH 30, 2011

Today the Judiciary Committee hears from Director Robert Mueller of the Federal Bureau of Investigation (FBI).

This fall, Director Mueller will complete his ten-year term overseeing the FBI. He took over just days before the attacks of September 11, 2001. Since then, he has overseen a major transformation of the Bureau. While the FBI continues to perform all the functions of a Federal law enforcement agency, it has also greatly increased its role in ensuring our national security. There have certainly been false starts and growing pains, but Director Mueller has managed this transformation of a large and well established agency with great professionalism and focus.

Perhaps most admirably, Director Mueller has aggressively pursued both law enforcement and national security objectives while maintaining a strong commitment to the values and freedoms we hold most dear as Americans. In commemorating the 100th anniversary of the FBI several years ago, Director Mueller said:

> "It is not enough to stop the terrorist – we must stop him while maintaining his civil liberties. It is not enough to catch the criminal – we must catch him while respecting his civil rights. It is not enough to prevent foreign countries from stealing our secrets – we must prevent that from happening while still upholding the rule of law. The rule of law, civil liberties, and civil rights – these are not our burdens. They are what make us better. And they are what have made us better for the past 100 years."

I agree. I have tried to advance these same objectives with carefully calibrated criminal justice legislation like the Justice For All Act, and national security legislation like the USA PATRIOT Act reauthorization proposal that recently passed through this Committee. It is gratifying that the Director of the FBI shares my commitment to working to keep all Americans safe, while preserving the values that make us Americans.

I also appreciate that the FBI has shown signs recently of real progress on issues vital to this Committee and to the country. Obviously, national security and counter-terrorism are central to the FBI's mission. It has been heartening to see recently a steady stream of important arrests of those who would do this country harm.

For instance, earlier this month, the FBI arrested Kevin Harpham for planning to bomb a march in honor of Martin Luther King Day in Spokane, Washington. Mr. Harpham reportedly had ties to white supremacist groups, and the plot he is accused of planning came dangerously close to succeeding. The results could have been devastating. I commend the FBI for making this arrest, which shows the continuing threat posed by domestic terrorism and makes very clear that no one ethnic group has a monopoly on terror.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.048

In the last Congress, we made great strides toward more effective fraud prevention and enforcement. I worked hard with Senator Grassley and others to craft and pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade. That important legislation added resources and statutory tools for effective prevention, detection, and enforcement of mortgage fraud and financial fraud. We also worked hard to ensure that both the healthcare reform legislation and Wall Street reform legislation passed last year included important new tools for cracking down on fraud. Senator Grassley and I are hard at work now on new legislation to provide greater support for aggressive enforcement of our fraud laws.

I am pleased to see that the FBI has been taking advantage of this heightened support for fraud enforcement, greatly increasing the number of agents investigating fraud, leading to more fraud arrests and greater fraud recoveries. I am glad that the FBI has also maintained its historic focus on combating corruption. I hope the Bureau will remain committed to cracking down on the kinds of fraud that contributed so greatly to our current financial crisis and on corruption that undermines Americans' faith in their democracy.

I have been heartened to see that the FBI's statistics continue to show reductions in violent crime nationwide despite the painful recession. I commend the FBI on its good work in combating violent crime. I hope that Congress will continue to provide urgently needed assistance to state and local law enforcement, which has been vital to keeping crime down throughout the country.

Of course, areas of major concern remain, including the FBI's continuing struggles with modernizing its technology and information-sharing systems. This Committee must continue its vigorous oversight. I hope that today's hearing will shed light on those areas where the FBI is continuing to excel, as well as those areas that need further attention.

I thank Director Mueller for returning to the Committee, for his responsiveness to our oversight efforts, and for his personal example and impressive leadership over the past decade in returning the FBI to its best traditions. I thank the hardworking men and women of the FBI and look forward to the Director's testimony.

#####

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.049

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

MARCH 30, 2011

STATEMENT FOR THE RECORD 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
MARCH 30, 2011

I. Introduction

Good morning, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to appear before the Committee today.

The FBI has never faced a more complex threat environment than it does today, whether one considers terrorism, espionage, cyber-based attacks, or traditional crimes. Indeed, during the past year, the FBI has faced an extraordinary range of national security and criminal threats.

There were last October's attempted bombings on air cargo flights bound for the United States from Yemen, directed by al Qa'ida in the Arabian Peninsula (AQAP). There was last May's attempted car bombing in Times Square, aided by Tehrik-e-Taliban in Pakistan (TTP). These two attempted attacks demonstrate how al Qa'ida's affiliates and allies have the intent to strike inside the United States.

We have also seen a number of terrorist plots by lone offenders, involving such possible targets as the home of former president George W. Bush; a Christmas-tree lighting ceremony in Portland; and subway stations in the Washington, D.C., Metro system.

There were the arrests last summer of ten Russian spies, known as "illegals," who secretly blended into American society, committed to the long-term goal of clandestinely gathering information for Russia. There was the disclosure of thousands of classified United States diplomatic cables and other documents by WikiLeaks. There was the cyber intrusion at Google as well as countless other cyber incidents that threaten to undermine the integrity of the Internet and to victimize the businesses and people who rely on it.

There were billion-dollar investment and mortgage frauds that undermined the financial system and victimized investors, homeowners, and ultimately taxpayers. There continued to be insidious health care scams involving false billings and fake treatments that endangered patients and fleeced government health care programs.

Continued violence on our Southwest Border led to the murder last March of an American consulate worker, her husband, and the spouse of another Consulate employee in

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.051

Juarez, Mexico, as well as the shooting last month of two U.S. Immigration and Customs Enforcement agents in Mexico.

And throughout, there were serious corruption cases that undermined the public trust, and violent gang cases that continued to endanger our communities.

As these examples demonstrate, the FBI's mission to protect the American people has never been broader or more complex, and the demands on the FBI have never been greater.

Since the 9/11 attacks, the FBI has transformed itself into a threat-driven, intelligence-led national security agency whose highest priority is to protect our nation from terrorist attack. But terrorism is by no means our only priority. We have also expanded our capabilities to confront the increased threat of cyber-based attacks, and we continue to maintain our responsibilities for combating public corruption, transnational organized crime, major white-collar crime, and significant violent crimes.

The FBI's transformation is an ongoing effort, and to meet all these challenges in the years to come, we will continue to need the full support of Congress.

II. Counterterrorism

Terrorism, in general, and al Qa'ida and its affiliates, in particular, continue to present the most significant threat to our national security. As we have seen in recent months, al Qa'ida and its affiliates remain committed to conducting attacks inside the United States, and they constantly develop new tactics and techniques to penetrate our security measures.

While the risk posed by core al Qa'ida is clear, organizations such as AQAP and TTP have emerged as significant threats, demonstrating both the intent and capability to attack the homeland as well as our citizens and interests abroad. Take, for example, the attempted 2009 Christmas Day airline bombing, which was directed by AQAP; or last May's failed Times Square car bombing, an attack linked to support from the TTP, a militant group in Pakistan. In each case, these groups were able to recruit individuals committed to attacking the United States, and whose backgrounds were less likely to trigger security scrutiny.

AQAP also took responsibility for directing the attempt last October to send two packages containing plastic explosives and detonators on air cargo flights bound from Yemen to the United States.

We also confront the increasing use of the Internet for spreading extremist propaganda, and for terrorist recruiting, training, and planning. Consider the impact of someone like Anwar Aulaqi – the Yemeni-based extremist. Fifteen years ago, Aulaqi's means of communication were limited. Today, on the Internet, he has unlimited reach to individuals around the world, including those here at home.

In the past ten years, al Qa'ida's online presence has become just as detrimental as its physical presence. As noted above, extremists are not limiting their use of the Internet to

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.092

recruitment or radicalization; they are using it to incite terrorism. Thousands of extremist websites promote violence to an online worldwide audience predisposed to the extremist message. They are posting videos on how to build backpack bombs and bio-weapons. They are using social networking to link terrorist plotters and those seeking to carry out these plans

Along with traditional international terrorist groups, homegrown terrorists, as well as domestic terrorist groups, also pose a serious, rapidly evolving threat. There is no typical profile of a homegrown terrorist; their experiences and motivating factors vary widely.

In December, an FBI sting led to the arrest of a 21-year-old man for an alleged plot to bomb a military recruiting center in Catonsville, Maryland. Last November, an FBI sting operation resulted in the arrest of a 19-year-old Somali-American student who allegedly attempted to detonate what he believed was a car bomb during a Christmas-tree lighting ceremony in Portland, Oregon. And last October the FBI arrested a Pakistani-American named Farooque Ahmed, who allegedly plotted to bomb subway stations in the Washington, D.C., Metro system.

The FBI also continues to see the phenomenon of American citizens who become radicalized and then travel overseas to take up arms with terrorist groups. A recent example is Zachary Chesser, a Virginia man arrested last July while attempting to travel to Somalia, where he intended to join the terrorist organization Al Shaabab as a foreign fighter. Last month he received a 25-year prison sentence. Another example is the "D.C. Five," a group of five young American men originally from Northern Virginia who traveled to Pakistan in late 2009. They were sentenced last June in Pakistan to ten years in prison on terrorism-related charges. These cases raise the question whether other such young men will one day return home to the United States, and, if so, what they might undertake here.

Finally, the FBI remains vigilant against the threat of attacks by domestic-based terror groups. In January, a pipe bomb was discovered during a Martin Luther King Day parade in Spokane, Washington. And last March, nine members of the Michigan-based Hutaree Militia were indicted for their alleged involvement in a plot to kill law enforcement officers and possibly civilians using illegal explosives and firearms.

In sum, we are seeing an increase in the sources of terrorism, a wider array of terrorist targets, and an evolution in terrorist tactics and means of communication – all of which makes the FBI's job that much more difficult. These terrorist threats are diverse, far-reaching, and ever-changing. Combating them requires the FBI to continue improving our intelligence and investigative programs, and to continue engaging our intelligence and law enforcement partners, both domestically and overseas. The FBI understands that protecting America requires the cooperation and understanding of the public. Since the 9/11 attacks, the FBI has developed an extensive outreach program to Muslim, South Asian, and Sikh communities to develop trust, address concerns, and dispel myths in those communities about the FBI and the U.S. government. As part of this effort, in 2009 the FBI established the Specialized Community Outreach Team (SCOT), composed of special agents, analysts, community outreach specialists, and personnel with language or other specialized skills. This team assists field offices with establishing new contacts in key communities.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.053

We encourage Congress to reauthorize the three critical FISA tools that will expire later this year: roving wiretap authority, access to business records under FISA and the "lone wolf" provision. Two of these tools have been part of FISA since the USA PATRIOT Act was enacted nearly a decade ago, and the third has been in FISA since 2004. They have all been reauthorized several times. Each facilitates the collection of vital foreign intelligence and counterintelligence information to support our national security mission.

III. Cyber Security

Cyber threats to our national security are broad in nature, from acts of terrorism supported by the use of the Internet, to economic espionage by foreign countries, to sophisticated state-sponsored hackers. Such threats could compromise our national critical infrastructure, from energy, water, telecommunications and transportation systems to financial services.

Cyber Threats

With regard to the terrorist use of the Internet, terrorists have not used the Internet to launch a full-scale cyber attack. But terrorist sympathizers have used the Internet to hide their communications, attempted denial-of-service attacks, and defaced numerous websites. And while the damage may have been limited, such groups may attack for publicity or impact, and they are becoming more adept at both.

The FBI, with our partners in the intelligence community, believes that the threat from the terrorist use of the Internet is a growing terrorist threat area. We speculate they will either train their own recruits or hire outsiders, with an eye toward leveraging physical attacks with use of the internet.

The cyber threat is equally significant with regard to counterintelligence intrusions and economic espionage. Today, our adversaries sit within our networks, often unknown and undetected. They may be nation-state actors or mercenaries for hire, rogue hackers or transnational criminal syndicates.

These hackers actively target both government and corporate networks. They seek our technology and our trade secrets, our intelligence and our intellectual property, even our military weapons and strategies.

The FBI is actively pursuing each of these threats. We have cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners. Together, they run complex undercover operations and examine digital evidence. They share information with our law enforcement and intelligence partners, including the Secret Service, which also has strong capabilities in this area. And they teach their counterparts – both at home and abroad – how best to investigate cyber threats.

But the FBI cannot do it alone. The National Cyber Investigative Joint Task Force includes 20 law enforcement and intelligence agencies, working side by side to share intelligence

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.054

and to identify key players and schemes. The goal is to predict and prevent what is on the horizon, and to pursue the enterprises behind these attacks. Last year's takedown of the Mariposa botnet is but one example of that collaboration. As you may know, Mariposa was an information-stealing botnet – one that infected millions of computers, including major banks and other Fortune 1000 companies. And this case, like so many others, emphasized the need for global cooperation. We look forward to working with Congress as it considers whether it should enact legislation requiring companies to report significant breaches of their network security to the FBI and other law enforcement agencies in real time. Such a requirement would promote coordination between appropriate agencies to investigate intrusions, identify the bad actors, and take actions to prevent further damage.

We have more than 60 FBI Legat offices around the world, sharing information and coordinating joint investigations with our host countries. And we have Special Agents embedded with police forces in Romania, Estonia, and the Netherlands, to name just a few. With our partners in the United Kingdom, Germany, and Turkey, we dismantled Darkmarket, one of the most sophisticated online criminal syndicates – and one of the forerunners in using the Internet to buy and sell stolen financial data. We must continue to press forward, country by country, and company by company.

Apart from the national security threat posed by cyber criminals, we confront traditional crime that has migrated and, indeed, flourished, on the Internet, from crimes against children to fraud.

Internet Fraud

With regard to Internet fraud, the 2010 Internet Crime Report was released in February. Last year, the Internet Crime Complaint Center (IC3) received more than 300,000 complaints of Internet crime, the second-highest total in IC3's history. The IC3 is a partnership between the FBI and the National White Collar Crime Center. Since its creation in 2000, IC3 has received more than two million Internet crime complaints.

Last year, IC3 referred more than 120,000 complaints to law enforcement for further investigation. New technology developed for IC3 enables investigators to share information and collaborate on cases that cross jurisdictions, as nearly all cyber crime cases do. IC3 analysts also provide support for investigative efforts.

The IC3 is a unique resource for federal, state, and local law enforcement to intake cases efficiently, find patterns in what might appear to be isolated incidents, combine multiple smaller crime reports into larger, higher priority cases, and ultimately bring cyber criminals to justice.

Innocent Images National Initiative

The Innocent Images National Initiative (IINI), a component of the FBI's Cyber Crime Program, is an intelligence-driven, multi-agency operation combating the proliferation of online child pornography and child exploitation. The mission of the IINI is to reduce the vulnerability of children to acts of sexual exploitation and abuse facilitated through computers; to identify and

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.055

rescue child victims; to investigate and prosecute sexual predators who use the Internet to exploit children for personal or financial gain; and to strengthen the capabilities of federal, state, local, and international law enforcement through training and investigative assistance.

From 1996 to 2009, child exploitation investigations in the FBI increased more than 2,500 percent. IINI currently has more than 6,000 child pornography cases. During FY2009 and FY2010, we made more than 2,000 arrests and obtained more than 2,500 convictions. We also identified 246 children exploited in child pornography in FY2010.

The Innocent Images International Task Force brings together law enforcement from around the world to prevent and prosecute online child exploitation. Currently, nearly 100 international officers from 42 countries participate on the task force, which allows for the real-time transfer of information and coordination of cases.

One such investigation, dubbed Operation Achilles, involved our partners in Australia, New Zealand, Canada, Belgium, Italy, and Britain. The three-year investigation uncovered suspects who traded more than 400,000 images of children, many depicting acts of violence and torture. Forty children were rescued, four websites were shut down, and 22 members of the ring were arrested. Fourteen of the 22 members were Americans who were successfully prosecuted by the Justice Department's Child Exploitation and Obscenity Section (Criminal Division) and the U.S. Attorney's Office for the Northern District of Florida.

Crimes Against Children

Child prostitution remains one of our most serious problems. In June 2003, the FBI, the Department of Justice Child Exploitation and Obscenity Section, and the National Center for Missing and Exploited Children joined forces to launch the Innocence Lost National Initiative (ILNI), targeting the growing problem of domestic sex trafficking of children in the United States. Each of the ILNI's 41 task forces and working groups throughout the United States include federal, state and local law enforcement agencies working in tandem with U.S. Attorney's Offices.

The FBI's Crimes Against Children Unit also coordinates an ongoing national sting operation entitled Operation Cross Country to combat domestic sex trafficking of children. ILNI task forces and working groups in 54 cities have participated in the operation by targeting venues such as the street tracks, truck stops, motels, and casinos where children are typically prostituted.

Through Operation Cross Country, more than 2,100 law enforcement officers have joined together to rescue child victims and apprehend those who victimize them. As a result, 248 child victims have been safely recovered during Operation Cross Country, phases I through V, and we have arrested 322 pimps engaged in the commercial sexual exploitation of children. For example, in November 2010, in Operation Cross Country V, the FBI and other agencies recovered 70 children and executed 885 arrests, including 99 pimps.

To date, the ILNI has resulted in more than 600 federal and state convictions and the location and recovery of more than 1,300 children. Together, we have obtained substantial

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.056

sentences for those convicted, including six life sentences and numerous others ranging from 25-45 years.

IV. Counterintelligence

The foreign intelligence threat to the United States continues unabated, from traditional means, such as last year's arrest of a network of Russian spies living in the United States, to more contemporary methods of tradecraft. Foreign intelligence services continue to target political and military intelligence, as well as information from economic institutions, both in and outside government. Foreign adversaries, however, do not rely on traditional agent networks alone – they are increasingly making use of non-traditional collectors, such as students, visiting scholars and scientists, and business people.

To counter this threat, the FBI relies on long-standing counterintelligence programs and methods. But we have also developed the National Strategy for Counterintelligence to deter and disrupt more modern counterintelligence threats. Its success relies heavily on strategic partnerships to determine and safeguard those technologies that, if compromised, would result in catastrophic losses to national security. Through our relationships with businesses, academia, and U.S. government agencies, the FBI and its counterintelligence partners can identify and effectively protect projects of great importance to the U.S. government.

With the ongoing WikiLeaks disclosure of classified information, we must also be concerned with insider threat capabilities to gather information for unauthorized disclosure.

The FBI began a review more than a year ago, not related to WikiLeaks events, of information and network access policies through its Information Sharing Policy Board, to better balance policies governing the "need to know" with the "responsibility to share." We wanted to ensure that FBI policy enabled appropriate internal and external sharing, and that statutory and Department of Justice guidance was applied throughout the FBI.

As a result, the FBI has reaffirmed its policy of restricting access to its classified networks and allowing direct access to FBI databases or internal share sites from external networks only when appropriate. We also maintain strict rules governing information sharing to protect the privacy of data related to U.S. persons across the different security and information domains. We have instituted strict enforcement of internal access to restricted data, ensuring information systems and discovery applications use the same access policies.

This past December, as a result of the WikiLeaks investigation, the FBI's Inspection Division began a review of policy compliance within the FBI, especially regarding access to restricted files. The Security Division issued a series of bulletins reminding employees of their responsibility to protect all information, and accelerated deployment of data protection mechanisms, including stricter enforcement of removable media use, the blocking of unauthorized devices, and increased monitoring of data movement throughout the Bureau.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.057

V. Criminal Programs

While national security remains our top priority, criminal programs are a key component of our core mission. And we must recognize that national security is as much about keeping our streets safe from crime as it is about protecting the United States from terrorist attack.

The Uniform Crime Report indicates that crime rates continue to fall in cities across the country. But these numbers may not necessarily reflect what we are seeing on our streets. We confront migrating gang activity, violence and corruption on the Southwest Border, international organized crime, white-collar crime, public corruption, and increasing sophistication in both mortgage fraud and health care fraud.

Financial crime, ranging from mortgage and health care fraud to corporate fraud and public corruption, continues to pose a significant threat to our financial systems. These frauds directly victimize millions of taxpayers, homeowners, shareholders, and everyday citizens alike.

Mortgage Fraud

In FY2010, we had more than 3,000 pending mortgage fraud investigations – compared to roughly 700 cases in 2005. Nearly 70 percent of those investigations exceed losses of more than $1 million each.

The FBI currently has 27 Mortgage Fraud Task Forces and 67 Mortgage Fraud Working Groups nationwide. With representatives of federal, state, and local law enforcement, these teams are strategically placed in mortgage fraud "hot spots" across the country. The FBI also has created the National Mortgage Fraud Team, which oversees the national mortgage fraud program, ensuring that we maximize limited resources, pinpoint the most egregious offenders, and identify emerging trends before they flourish. We must also continue to raise public awareness of mortgage fraud schemes, to better prevent fraud in the first place.

Health Care Fraud

The focus on health care fraud is no less important. The federal government spends hundreds of billions of dollars every year to fund Medicare and other government health care programs, and taxpayers rightly expect these funds to be used to provide health care to senior citizens, children, low-income individuals, and disabled individuals. Most medical professionals, providers, and suppliers work hard to comply with the rules. But too many in the health care industry commit schemes that cheat taxpayers and patients alike, and defraud Medicare and other government programs.

Together with our partners in the Department of Justice and the Department of Health and Human Services, the FBI is fighting back. In FY2010, we recovered a record $4 billion on behalf of taxpayers. This represents an approximate $1.47 billion, or 57 percent, increase over the amount recovered in FY2009, which was itself a record amount. Indeed, over the past three years, we have collectively recovered an average of nearly $7 for every dollar expended. In FY2010, the Department of Justice brought criminal health care fraud charges against 931

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.098

defendants, the most ever in a single fiscal year, and we obtained 726 convictions, also a record. And the FBI continues to investigate nearly 2,600 cases of health care fraud.

For example, in February 2011, the Medicare Fraud Strike Force – a partnership between the Department of Justice and the Department of Health and Human Services – charged more than 100 defendants in nine cities, including doctors, nurses, health care companies, and executives, for their alleged participation in Medicare fraud schemes involving more than $225 million in false billing. By all accounts, this stands as the largest federal health care fraud takedown in history.

But these strike forces are only part of the FBI's overall health care fraud efforts. The FBI is the only government investigative entity with jurisdiction over both public and private health care programs, and we are uniquely positioned to investigate a broad spectrum of health care fraud activity. From those who defraud Medicare to individuals committing complex schemes against private insurers such as we saw committed against AFLAC in 2010. Agents and analysts are using intelligence to identify emerging schemes; they are developing new techniques to help mitigate the threat. We are using undercover operations and wiretaps, not only to collect evidence for prosecution, but to cut off the heads of these criminal enterprises so they cannot flourish elsewhere. We have dismantled dozens of criminal enterprises engaged in widespread health care fraud, and we have sought seizures and forfeitures to recover program funds.

Corporate Fraud

The FBI and its law enforcement partners continue to uncover major frauds and Ponzi schemes. At the end of FY2010, the FBI had more than 2,300 active corporate and securities fraud investigations.

In December 2010, President Obama's interagency Financial Fraud Enforcement Task Force (FFETF) announced the results of Operation Broken Trust, which highlighted the prevalence of a wide range of investment fraud schemes around the country during a three-and-a-half month period. This enforcement effort included investigations with hundreds of defendants who committed fraud schemes involving more than 120,000 victims and estimated losses totaling more than $8 billion.

With regard to high-level executive prosecutions, a few notable cases highlight our commitment to finding and convicting those individuals who may have contributed to the recent financial crisis.

In June 2010, Lee Farkas, former chairman of Taylor, Bean, and Whitaker (TBW), a large mortgage origination company, was charged with a $1.9 billion fraud that contributed to the failure of Colonial Bank, one of the largest banks in the United States and the sixth largest bank failure in the country. His trial is scheduled for later this year. On March 2, 2011, Catherine Kissick, a former senior vice president of Colonial Bank and head of its Mortgage Warehouse Lending division, pled guilty to conspiring to commit bank, wire, and securities fraud. She faces a maximum sentence of 30 years in prison. And on February 24, 2011, Desiree

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.059

Brown, the former treasurer of TBW, pled guilty to conspiring to commit bank, wire, and securities fraud for her role in this fraud scheme.

On February 25, 2011, Michael McGrath, former President and Owner of U.S. Mortgage Corporation, formerly one of the largest private residential mortgage companies in New Jersey, was sentenced to 14 years in prison for his role in perpetrating a corporate fraud scheme involving the double selling of mortgage loans to Fannie Mae, which resulted in losses in excess of $100 million. And in October 2010, Jeffrey Thompson, former President of Hume Bank, pled guilty to making false statements to the FDIC as part of a bank fraud scheme that caused such significant losses that the bank was pushed into insolvency. Thompson faces a sentence of up to 30 years in federal prison without parole, plus a fine up to $1 million and an order of restitution.

These are just a few examples of the thousands of financial fraud investigations ongoing at the FBI and conducted in conjunction with the administration's Financial Fraud Enforcement Task Force.

Public Corruption

The FBI recognizes that fighting public corruption is vital to preserving our democracy, protecting our borders, and securing our communities. Indeed, public corruption remains our top criminal priority.

On October 10, 2010, 89 law enforcement officers and 44 others were arrested and charged in Puerto Rico as part of Operation Guard Shack, the largest police corruption investigation in the history of the FBI. Close to 750 FBI agents were flown in to Puerto Rico from across the country to assist in the arrests. This two-year multi-jurisdictional, multi-agency operation sent a powerful message – that corruption among our public officials will not be tolerated.

The FBI is also working to confront international contract corruption. The FBI's Criminal Investigative Division joined with our federal law enforcement partners to stand up the International Contract Corruption Task Force (ICCTF), which includes all fraud against the U.S. government where the illegal conduct occurred outside the United States and involves United States persons or funds. Since 2004, the ICCTF has initiated nearly 800 investigations in Afghanistan, Iraq, and Kuwait.

For example, in December 2009, Major John Lee Cockerham, Jr., a former U.S. Army contracting officer, was sentenced to more than 17 years for his participation in a bribery and money-laundering scheme related to bribes paid for contracts awarded in support of the Iraq war. Cockerham was convicted of receiving favors, cash, and items of value from contractors in exchange for favorable treatment and consideration on contracts awarded in Iraq and Kuwait. Once he agreed to take money in exchange for awarding contracts, Cockerham directed the contractors to pay his wife, sister, and others to hide the fact that contractors were paying bribes. His wife has since been sentenced to 41 months in prison. His sister received 70 months for her role in the scheme. The total restitution orders included more than $14 million.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.080

As Assistant Attorney General Lanny Breuer noted in his January 2011 testimony before the Senate Judiciary Committee, the Department of Justice and the FBI is also steadfastly pursuing corporate corruption and bribery in violation of the Foreign Corrupt Practices Act ("FCPA"). This corruption and bribery works to the detriment of us all, undermining the transparency and honesty of corporate culture. In 2010, we recovered over $1 billion through resolutions of FCPA investigations, more than in any other year in the history of our FCPA enforcement efforts.

Gang Violence

Every day, violent gangs infiltrate new neighborhoods, new schools, and new street corners. Gangs are no longer limited to urban areas, but have migrated to more rural settings, from Billings, Montana, and Salt Lake City, Utah, to Charlotte, North Carolina, and Omaha, Nebraska. Gangs have also infiltrated our prisons and even the military. Gangs have diversified from drug running and petty crime to armed robbery, home invasions, mortgage and health care fraud, even human trafficking. The economic impact of their criminal activity is estimated to be $5 billion each year.

We have over 230 Violent Gang, Safe Streets, and Safe Trails Task Forces across the country. Through these task forces, we identify and target major groups operating as criminal enterprises. Much of our intelligence comes from our state and local law enforcement partners, who know their communities inside and out. We are using enhanced surveillance and embedded sources to track these gangs, and to identify emerging trends. In the past six months, we have arrested more than 3,500 gang members. To date, we have obtained more than 1,400 convictions. And we have recovered roughly $19 million in forfeitures and seizures. Additionally, the FBI is a strong participant in GangTECC, a DOJ multiagency gang coordination initiative.

By conducting these multi-subject and multi-jurisdictional investigations, the FBI can concentrate on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

Organized Crime

We are also concerned with the increased presence and impact of international organized criminal enterprises. Some believe that organized crime is a thing of the past. Unfortunately, this is not the case. Traditional criminal syndicates still con, extort, and intimidate American citizens. On January 20, 2011, we arrested nearly 130 members of La Cosa Nostra in New York, New Jersey, and New England. And we will continue to work with our state and local partners to end La Cosa Nostra's lifelong practice of crime and undue influence.

But we have seen a shift from regional families with clear structures to flat, fluid networks with global reach. These international enterprises are running multi-national, multi-billion dollar schemes from start to finish. In an October 13, 2010, health care fraud takedown, 73 members and associates of organized crime groups (for example, Mirzoyan-Terdjanian Organization) were among those indicted for more than $163 million in health care fraud

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.061

crimes. Among the defendants charged is Armen Kazarian, who is alleged to be a "Vory-V-Zakone," a term translated as "Thief-in-Law" and referring to a member of a select group of high-level criminals from Russia and the countries previously part of the former Soviet Union, including Armenia.

On September 16, 2010, 44 members of a Chinese/Korean criminal enterprise involved in a highly sophisticated fraudulent document and identity theft operation were arrested in New Jersey and New York. The charges included aggravated identity theft, passport fraud, bank fraud and tax evasion. The investigation was spawned by a Chicago investigation, which resulted in arrests of 30 members of an Asian criminal enterprises involved in the manufacture and distribution of "identity sets." Each identity set consists of an altered People's Republic of China passport and an authentic SSN. DHS estimates the actual damage inflicted by the "586" fraud network to be in the vicinity of $400 to 500 million since mid-2006, reflecting a significant economic impact on citizens and financial institutions in the United States.

We are also taking a hard look at other groups around the world, including West African and Southeast Asian organized crime. We are sharing that intelligence with our partners who, in turn, will add their own information. The goal is to combine our resources and our expertise to gain a full understanding of each group, and to better understand what we must do, together, to put them out of business. The FBI is also contributing to this end through its participation in the International Organized Crime Intelligence Operations Center (IOC).

Violence and Corruption Along the Southwest Border

The U.S. border with Mexico extends nearly 2,000 miles, from San Diego, California, to Brownsville, Texas. At too many points along the way, drug cartels transport kilos of cocaine, methamphetamine, heroin, and marijuana, gangs kidnap and murder innocent civilians, traffickers smuggle human cargo, and corrupt public officials line their pockets by looking the other way – any one of these offenses represents a challenge for law enforcement. The severity of this problem is highlighted by the following statistics:

- Between 18 and 39 billion dollars flow annually from the United States across the Southwest Border to enrich the Mexican drug cartels.
- Over 3,000 drug-related murders in Juarez, Mexico, in 2010.
- Over 34,600 drug-related murders in all of Mexico from December 2006 to December 2010.
- Estimated that 95 percent of all South American cocaine that moves from South America to the United States goes through Mexico.
- 701,000 kilograms of marijuana were seized during the first five months of 2010 in Arizona, California, New Mexico, and Texas.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.082

To address corruption on the Southwest border, we have 13 border corruption task forces with roughly 120 agents in FBI field offices in the region, and one National Border Corruption Task Force at FBI Headquarters to direct these efforts. We have border liaison officers who work one-on-one with their law enforcement counterparts in Mexico.

To address security along the Southwest Border, we have developed an intelligence-led, cross-programmatic strategy to penetrate, disrupt and dismantle the most dangerous organizations and bring top criminals to justice. This strategy begins with the deployment of hybrid squads in hot spots throughout the area, from Albuquerque, El Paso, and San Antonio, to Dallas, Phoenix, and San Diego.

The goal of the hybrid squad model is to bring expertise from multiple criminal programs into these dynamic, multi-faceted threats and then target, disrupt, and dismantle these organizations. Hybrid squads consist of multi-disciplinary teams of Special Agents, Intelligence Analysts, Staff Operations Specialists, and other professionals. The agent composition on the squads provides different backgrounds and functional expertise, ranging from gang activity and violent crime to public corruption.

Our first success with these hybrid squads came in July 2010, with Operation Luz Verde, which resulted in the arrest of 43 individuals affiliated with the Arellano Felix drug trafficking organization, including a high-ranking official in the Baja Attorney General's Office.

The recent focus on Barrio Azteca, one of the narcotics-focused gangs responsible for the violence in cities like Juarez, Mexico, illustrates this approach. Barrio Azteca has been tied to drug trafficking, prostitution, extortion, assaults, murder, and the retail sale of drugs. Most recently, the gang was linked to the murder of a U.S. Consulate employee, her husband, and the spouse of another Consulate employee in Juarez.

The FBI has been working closely with DHS in a joint effort to investigate the attack against two ICE special agents in Mexico on February 15, 2011, by suspected members of a Mexican drug trafficking organization. Jaime Zapata and Victor Avila were ambushed while traveling from Matehuala, Mexico, to Mexico City in an armored vehicle with diplomatic license plates. Agent Zapata was killed in the attack. The Department of Justice created a joint task force to investigate these shootings, with the FBI as the lead task force agency. On February 24, 2011, Mexican law enforcement detained six individuals in connection with the shooting.

Indian Country

The FBI has the primary federal law enforcement authority for felony crimes in Indian Country. Even with demands from other threats, Indian Country law enforcement remains a priority for the FBI. Last year, the FBI handled more than 2,400 Indian Country investigations throughout the country.

Approximately 75 percent of all FBI Indian Country investigations involve homicide, crimes against children, or felony assaults. Available statistics indicate that American Indians and Alaska Natives suffer violent crime at far greater rates than other Americans. Violence

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.083

against Native women and children is a particular problem, with some counties facing murder rates against Native women well over 10 times the national average.[1] In addition to violence, there is a significant emerging threat from fraud and other white-collar crimes committed against tribally run gaming facilities.

Currently, the FBI has 18 Safe Trails Task Forces focused on drugs, gangs and violent crimes in Indian Country. The gang threat on Indian reservations has become evident to the tribal community leaders, and gang related violent crime is reported to be increasing. Tribal community leaders have reported that some youth are bringing back gang ideology from major cities, and Drug Trafficking Organizations are recruiting tribal members.

The FBI's Indian Country Special Crimes Unit works with the Bureau of Indian Affairs Office of Justice Services to sponsor and promote core training for investigators. The FBI provides training for state, local, tribal, and federal investigators regarding gang assessment, crime scene processing, child abuse investigations, forensic interviewing of children, homicide investigations, interviewing and interrogation, and Indian gaming. Furthermore, the FBI's Office of Victim Assistance dedicates a significant number of Victim Specialists to Indian Country to assist the victims of these crimes.

Information Technology

The FBI continues to improve how we collect, analyze, and share information using technology. Intelligence provides the information we need, but technology further enables us to find the patterns and connections in that intelligence. Through sophisticated, searchable databases, we are working to track down known and suspected terrorists through biographical information, travel histories and financial records. We then share that information with those who need it, when they need it.

Earlier this month, the FBI's Criminal Justice Information Services division started using the Next Generation Identification (NGI) System – new technology that will enhance our ability to more quickly and efficiently identify criminals and terrorists, here at home and around the world. With NGI, we are incrementally replacing the Integrated Automated Fingerprint Identification System, which provides automated fingerprint and latent search capabilities to more than 18,000 law enforcement and criminal justice partners, 24 hours a day, 365 days a year. With this new technology, we will have the ability to process fingerprint transactions much faster and with more accuracy.

We are also working to better integrate data sets throughout the Bureau. For example, the FBI has developed the Data Integration and Visualization System (DIVS), with the goal to prioritize and more effectively integrate nearly 200 datasets across the Bureau. The FBI currently has investigative data that is stored and accessed in multiple systems. As a consequence, our personnel are spending too much time hunting for data, leaving them less time to analyze that data to stay ahead of threats.

---

[1] Zaykowki, Kallmyer, Poteyeva & Lanier (Aug. 2008), *Violence Against American Indian and Alaska Native Women and the Criminal Justice Response: What is Known*, Bachman (NCJ # 223691), at 5, http://www.ncjrs.gov/pdffiles1/nij/grants.223691.pdf.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.064

DIVS provides single sign-on, role-based access controls to analyze and link all FBI data that the user is lawfully allowed to see and will provide the means to efficiently feed FBI Secret data to the FBI Top Secret system. DIVS will not only significantly improve users' efficiency in searching multiple databases, it will ultimately help reduce or eliminate redundant data systems.

Finally, I would like to touch on the Sentinel program. The first two phases of the Sentinel case management system have been deployed and are used by thousands of agents, analysts, and supervisors to access, retrieve, and manage information necessary for FBI operations. The FBI is using agile software development processes to build on the existing program and complete the additional capabilities and functionality of Sentinel.

The Sentinel development team is working in two-week sprints to finish the project. Every two weeks, new capabilities are demonstrated to the FBI's senior executives, with formal monthly updates to the Department of Justice. These smaller development teams provide more flexibility in prioritizing our requirements, incorporating user feedback more quickly and meeting our goals, step by step. The next significant functions are scheduled to be in place in April 2011, with Sentinel scheduled to be operational in September 2011.

One lesson we have learned in recent years is the need to ensure that as new technology is introduced into the marketplace, the FBI and its law enforcement partners maintain the technical capabilities to keep pace. In the ever-changing world of modern communications technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to a court order and our practical ability to actually intercept those communications.

As the gap between authority and capabilities widens, the Federal government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage – evidence that a court has authorized us to collect. We need to ensure that our capability to execute lawful court orders to intercept communications does not diminish as the volume and complexity of communications technologies expand.

Similarly, our investigations can be stymied by the records preservations practices of private communications providers. Current law does not require telephone companies and Internet service providers to retain customer subscriber information and source and destination data for any set period of time. This has resulted in an absence of data that may hinder crucial evidence in a child exploitation cases, terrorism, online piracy, computer hacking, and other privacy-related crimes, for example. We look forward to continuing to work with Congress as it considers whether legal changes are needed, and to ensure that any such changes are narrowly tailored to provide targeted government access to information consistent with the protection of privacy and civil liberties.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.085

Conclusion

I appreciate the opportunity to review some of the FBI's recent work responding to the complex and far-ranging threats we face today. I also want to thank the Committee for your continued support of the FBI's mission, which has been essential to our ability to meet these diverse challenges. We will continue to need your support to complete the Bureau's transformation and to meet the full responsibilities of our mission.

I look forward to working with the Committee during the remainder of my tenure as Director to improve the FBI and strengthen its ability to keep the nation safe. I would be happy to answer any questions that you may have.

VerDate Nov 24 2008 09:09 Jan 05, 2012 Jkt 071557 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\71557.TXT SJUD1 PsN: CMORC

71557.086

Nielsen//NetRatings A global leader in Internet media and market research

For Immediate Release:
NetRatings, Inc.

Suzy Bausch (408) 941-2965

NIELSEN//NETRATINGS REPORTS TOPLINE U.S. DATA FOR JULY 2007

Nielsen//NetRatings reports July 2007 data for the Top Sites by Parent Company and Top Brands. In addition, Nielsen//NetRatings reveals the Top Advertisers by Company for July 2007.

Nielsen//NetRatings Top 10 Web Sites by Parent Company and Top 10 Web Sites by Brand, July 2007

Table 1. Top 10 Parent Companies, Combined Home & Work (U.S.)

Parent	Unique Audience (000)	Time Per Person (hh:mm:ss)
1. Microsoft	121,499	2:07:26
2. Google	117,705	1:34:07
3. Yahoo!	111,390	2:58:43
4. Time Warner	104,946	4:05:58
5. News Corp. Online	76,705	2:26:30
6. eBay	68,203	1:44:26
7. InterActiveCorp	61,580	0:22:03
8. Amazon	50,747	0:26:23
9. Wikimedia Foundation	44,763	0:18:20
10. New York Times Company	44,704	0:15:43

Table 2. Top 10 Brands, Combined Home & Work (U.S.)

Brand	Unique Audience (000)	Time Per Person (hh:mm:ss)
1. Google	111,609	1:08:08
2. Yahoo!	110,377	2:59:13
3. MSN/Windows Live	100,523	1:56:02
4. Microsoft	94,247	0:40:19
5. AOL Media Network	91,919	4:16:36
6. Fox Interactive Media	68,421	2:36:02
7. eBay	59,835	1:46:03
8. YouTube	55,135	0:49:59
9. Wikipedia	44,639	0:18:12
10. Amazon	43,090	0:23:44

Example: The data indicates that 44.7 million home and work Internet users visited at least one of the New York Times Company-owned sites or launched an New York Times Company-owned application during the month, and each person spent, on average, a total of 15 minutes and 43 seconds at one or more of their sites or applications.

A parent company is defined as a consolidation of multiple domains and URLs owned by a single entity. A brand is defined as a consolidation of multiple domains and URLs that has a consistent collection of branded content.

Nielsen//NetRatings AdRelevance Top 10 Advertisers, July 2007

Top advertisers, ranked by estimated spending, are based on data from AdRelevance, Nielsen//NetRatings' advertising research service. An impression is counted as the number of times an ad is rendered for viewing.

Top 10 Advertisers by Estimated Spending (U.S.)

Advertiser	Total Estimated Spending	Impressions (000)
1. Low Rate Source	$46,321,200	22,059,921
2. NexTag, Inc.	$43,715,300	21,409,913
3. Experian Group Limited	$43,405,900	15,674,399
4. Countrywide Financial Corporation	$34,776,800	17,091,495
5. InterActiveCorp	$27,873,800	6,784,473
6. Netflix, Inc.	$18,813,600	5,572,255
7. AT&T Corp.	$18,241,000	5,681,139
8. Privacy Matters	$16,878,100	5,558,021
9. Verizon Communications, Inc.	$15,715,000	4,016,248
10. Reunion.com L.L.C.	$14,113,300	6,830,167

Nielsen//NetRatings **A global leader in Internet media and market research**

Estimated spending reflects CPM-based advertising online, and excludes search-based advertising, paid fee services, performance-based campaigns, sponsorships, barters, partnership advertising, advertorials, promotions and e-mail. Impressions reported exclude house ads, which are ads that run on an advertiser's own or related property and co-branding relationships.

Example: An estimated 6.8 billion Reunion.com L.L.C. ads were rendered for viewing at the cost of approximately $14.1 million during the surfing period.

About Nielsen//NetRatings
Nielsen//NetRatings, a service of The Nielsen Company, delivers leading Internet media and market research solutions. With high quality, technology-driven products and services, Nielsen//NetRatings is the global standard for Internet audience measurement and premier source for online advertising intelligence, enabling clients to make informed business decisions regarding their Internet and digital strategies. The Nielsen//NetRatings portfolio includes panel-based and site-centric Internet audience measurement services, online advertising intelligence, user lifestyle and demographic data, e-commerce and transaction metrics, and custom data, research and analysis. For more information, please visit www.nielsen-netratings.com.

###

Editor's Note: Please source all data to Nielsen//NetRatings.

Nielsen//NetRatings **A global leader in Internet media and market research**

For Immediate Release:
NetRatings, Inc.

Suzy Bausch (408) 941-2965

NIELSEN//NETRATINGS REPORTS TOPLINE U.S. DATA FOR AUGUST 2007

Nielsen//NetRatings reports August 2007 data for the Top Sites by Parent Company and Top Brands. In addition, Nielsen//NetRatings reveals the Top Advertisers by Company for August 2007.

Nielsen//NetRatings Top 10 Web Sites by Parent Company and Top 10 Web Sites by Brand, August 2007

Table 1. Top 10 Parent Companies, Combined Home & Work (U.S.)

Parent	Unique Audience (000)	Time Per Person (hh:mm:ss)
1. Microsoft	118,058	2:11:23
2. Google	116,939	1:40:44
3. Yahoo!	110,651	3:20:53
4. Time Warner	106,626	3:56:00
5. News Corp. Online	74,803	2:23:27
6. eBay	67,275	1:48:31
7. InterActiveCorp	60,294	0:24:48
8. Amazon	50,809	0:27:37
9. Walt Disney Internet Group	46,208	0:37:13
10. Wikimedia Foundation	45,228	0:16:35

Table 2. Top 10 Brands, Combined Home & Work (U.S.)

Brand	Unique Audience (000)	Time Per Person (hh:mm:ss)
1. Google	111,165	1:12:40
2. Yahoo!	109,741	3:21:17
3. Microsoft	95,221	0:42:43
4. MSN/Windows Live	94,497	2:00:58
5. AOL Media Network	92,533	4:09:20
6. Fox Interactive Media	66,103	2:32:35
7. eBay	60,114	1:46:59
8. YouTube	56,453	0:53:37
9. Wikipedia	44,957	0:16:30
10. Amazon	42,675	0:24:54

Example: The data indicates that 45.2 million home and work Internet users visited at least one of the Wikimedia Foundation-owned sites or launched a Wikimedia Foundation-owned application during the month, and each person spent, on average, a total of 16 minutes and 35 seconds at one or more of their sites or applications.

A parent company is defined as a consolidation of multiple domains and URLs owned by a single entity. A brand is defined as a consolidation of multiple domains and URLs that has a consistent collection of branded content.

Nielsen//NetRatings AdRelevance Top 10 Advertisers, August 2007

Top advertisers, ranked by estimated spending, are based on data from AdRelevance, Nielsen//NetRatings' advertising research service. An impression is counted as the number of times an ad is rendered for viewing.

Top 10 Advertisers by Estimated Spending (U.S.)

Advertiser	Total Estimated Spending	Impressions (000)
1. Low Rate Source	$51,670,100	25,076,624
2. NexTag, Inc.	$49,627,300	23,614,378
3. Experian Group Limited	$40,895,600	14,891,457
4. InterActiveCorp	$35,537,500	8,842,437
5. Countrywide Financial Corporation	$35,442,800	17,380,341
6. AT&T Corp.	$29,774,300	10,748,844
7. Netflix, Inc.	$29,691,100	9,071,800
8. Verizon Communications, Inc.	$19,487,900	4,949,850
9. Monster Worldwide, Inc.	$17,355,500	3,264,426
10. Privacy Matters	$14,336,600	4,728,581

Nielsen//NetRatings **A global leader in Internet media and market research**

Estimated spending reflects CPM-based advertising online, and excludes search-based advertising, paid fee services, performance-based campaigns, sponsorships, barters, partnership advertising, advertorials, promotions and e-mail. Impressions reported exclude house ads, which are ads that run on an advertiser's own or related property and co-branding relationships.

Example: An estimated 4.7 billion Privacy Matters ads were rendered for viewing at the cost of approximately $14.3 million during the surfing period.

About Nielsen//NetRatings
Nielsen//NetRatings, a service of The Nielsen Company, delivers leading Internet media and market research solutions. With high quality, technology-driven products and services, Nielsen//NetRatings is the global standard for Internet audience measurement and premier source for online advertising intelligence, enabling clients to make informed business decisions regarding their Internet and digital strategies. The Nielsen//NetRatings portfolio includes panel-based and site-centric Internet audience measurement services, online advertising intelligence, user lifestyle and demographic data, e-commerce and transaction metrics, and custom data, research and analysis. For more information, please visit www.nielsen-netratings.com.

###

Editor's Note: Please source all data to Nielsen//NetRatings.