AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 111–1001

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JULY 28, 2010

Serial No. J–111–103

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
66–825 PDF WASHINGTON : 2011

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 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ARLEN SPECTER, Pennsylvania
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
AL FRANKEN, Minnesota

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

BRUCE A. COHEN, *Chief Counsel and Staff Director*
BRIAN BENCZKOWSKI, *Republican Chief Counsel*

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	90
Sessions, Hon. Jeff, a U.S. Senator from the State of Alabama	3

WITNESSES

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 Feinstein, Feingold, Durbin, Whitehouse, Kaufman, Franken, Sessions, Grassley and Kyl	44

SUBMISSIONS FOR THE RECORD

Mueller, Robert S., III, Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC:	
Correction of Misstatement	92
Responses from March 5, 2008, FBI Oversight Hearing	94

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

WEDNESDAY, JULY 28, 2010

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

The Committee met, pursuant to notice, at 10:01 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Kohl, Feinstein, Specter, Schumer, Durbin, Cardin, Whitehouse, Klobuchar, Kaufman, Franken, Sessions, Hatch, Grassley, and Kyl.

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

Chairman LEAHY. Good morning, everyone. I came out and I thought that Senator Sessions was out here, but it is your white hair I saw. But I understand he is on his way, and I am going to begin, and he will be recognized when he gets here.

The Judiciary Committee today hears from Director Robert Mueller of the FBI for the fourth time this Congress. We held two FBI oversight hearings last year, and the Director appeared earlier this year to testify about national security issues. I welcome him back to the Committee.

I would note the Director, the same as with his predecessor, has always been available anytime I have called or had questions. We have done briefings on both unclassified and classified matters, and I appreciate that and I appreciate his candor in responding. I wish I could talk about some of the things he has responded, but they were highly classified so I will not. But I just want to note for the record I appreciate his candor in that.

Oversight is one of our most important responsibilities, and this Committee has taken it very seriously. Along with regular appearances from Director Mueller, the Committee has held multiple oversight hearings with Attorney General Holder, oversight hearings with Homeland Security Secretary Napolitano, the heads of key components of the Justice Department, and other senior executive branch officials. And the FBI, of course, has a critical mission in law enforcement and national security. And the Director has been very open in his efforts to balance the efforts in law enforcement while maintaining the values and the freedoms that we hold dear as Americans. He has worked to close the longstanding gaps in responses to written questions, inquiries, and document requests from this Committee. We always want more work on that, but the

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

increased openness and responsiveness from the FBI helps the Bureau and Congress do their jobs more effectively. I would say that is helpful both as a member of this Committee and as a member of the Appropriations Committee.

I appreciate that they has shown signs recently of real progress on issues vital to this Committee and to the country. Obviously, national security and counterterrorism are central to the FBI's mission. It has been heartening to see in recent months a series of important arrests of those who would do this country harm, and, Director Mueller, I appreciate your briefings you have given me on those arrests.

But, also, last week the FBI announced the arrest of Zachary Chesser, an American who sought to join a terrorist organization in Somalia. Now, we see the headlines of arresting him, but what it does not show is the months and months of work, some of the finest investigative work I have seen, of FBI agents, and I hope you will compliment those agents who have followed him for months.

It appears from court documents and public statements that in this case the system worked as it should. Mr. Chesser was watched carefully through court-approved surveillance, was placed on the no-fly list, and was arrested as he tried to fly to Africa. Cases like these reinforce my conviction that criminal investigations and prosecutions are vital weapons in our national security arsenal.

In this Congress, we have made great strides toward more effective fraud prevention and enforcement. I worked hard with Senator Grassley, Senator Kaufman, and others to pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade. I was pleased when the President signed it into law last spring. I know Senator Kaufman was, too.

That important legislation added resources and statutory tools for effective prevention, detection, and enforcement of mortgage fraud and financial fraud. The same bipartisan group of Senators worked hard this year to ensure that the landmark health care reform legislation included new tools for cracking down on health care fraud, and that the historic Wall Street reform legislation the President just signed included key measures to strengthen enforcement of securities fraud and bank fraud.

I am glad to see that the FBI has been taking full advantage of this heightened support for and focus on fraud enforcement. This spring, the Attorney General told Congress that, in part as a result of the recently passed legislation, the FBI has more than doubled the number of agents investigating fraud, but that also reflects from the top, from the Director of the FBI, what he feels.

Since 2007, the Justice Department's health care fraud strike forces have sent more than 205 defendants to prison. They have significantly deterred Medicare fraud. That is one of the things that I know Senator Grassley and I have looked at very closely. And earlier this month, the Department charged 92 defendants with cheating the Medicare system of more than $251 million in the largest health care fraud sting ever. Senator Sessions and I, as former prosecutors, know that the way you deter some of these things is to deter them, actually lock them up. I congratulate the Director for the FBI's central role in these investigations. I hope they remain committed to that.

Combating corruption has long been another important priority for the FBI. I was very disappointed that the Supreme Court last month undermined these efforts by siding with Enron executive Jeffrey Skilling and greatly limiting a statute, passed with bipartisan support, vital to Federal efforts to crack down on corruption and fraud. And I have already spoken with the Director and hope he will work with us on both sides of the aisle to see if we can fix that statute to give him the tools he needs.

I am heartened to see that the FBI's statistics continue to show reductions in violent crime nationwide despite the painful recession. I commend them on their work in combating violent crime. But I also hope that Congress continues to supply and does supply the kind of resources you need to combat crime. It is one thing to say we will put the laws on the books and increase the penalties, but if we do not give you agents to go out and catch the people, it does not do much good.

Areas of major concern remain, of course. I know the FBI is continuing to struggle with efforts to modernize its technology and information-sharing systems. The Sentinel program, there will be questions about that because of the great concern I have expressed to you privately.

I was distressed to learn that the FBI has felt it necessary to suspend work orders and essentially start over yet again. I am glad to see you are taking control of it, but I am sorry we have gotten to that point. And I have also discussed with the Director the press reports this morning about widespread allegations of cheating on a test that is meant to ensure that FBI agents understand the limits of their investigative authorities, and I know the Director—it seems these stories always break the night before you are about to testify, but it will give us something—we want to make the hearing interesting for you, Director.

I thank you for returning. I also thank the hard-working men and women of the FBI. You have stated publicly your pride in these agents, but you have also told me privately the same. It is not something you just say in public. You say it privately, too, the pride you have in the men and women of the Bureau. I share that price.

Senator Sessions.

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

Senator SESSIONS. Thank you, Mr. Chairman. It is great to have Director Mueller, who is one of our Government's finest public servants, I think. But I do not think he would claim to be perfect, and the fabulous FBI is not perfect either, and we need to insist that we do all we can to assist you in making that great agency better than it is.

I would just say first this Government is spending money in ways we have never comprehended before. The last two budgets that passed this Congress increased domestic spending about 17 percent in each agency. That does not count the $800 billion stimulus package that is moving grant money out all over the country, and I continue to hear problems of fraud and abuse in that area.

In addition, the Government has assumed greater control than ever in the history of the world over our health care system, and it is going to cost the American people money. And it has got to be managed correctly.

I am concerned about that. We have got to have increased and more effective oversight over Federal spending as it grows, if for no other reason than it is growing in real terms. And so we need to focus more on that.

I was disappointed to see in general FBI fraud statistics are down. I do not think that is an acceptable trend in light of the American people's concern over waste, fraud, and abuse in the Federal Government.

Also, Mr. Director, I was a bit taken aback that we just got yesterday, perhaps, the answers to the written questions that I posed concerning the policy of the FBI when they arrest a terrorist, whether or not they will be presumptively a civilian defendant, if charged, or whether or not they would be handled by a military commission presumptively. And it appears that it remains the policy of this administration—I do not know what position you have personally taken, but the administration and the Department of Justice has apparently continued to pursue the view that these individuals, if arrested, like the Christmas Day bomber, are presumed to be tried in Federal civilian court, which means they are entitled to a prompt appearance before a magistrate, as you noted in your answers, given Miranda warnings, given pre-trial discovery, and given speedy trial rights; whereas, if they are treated as an enemy combatant, someone who has been arrested in the same way that German soldiers may have been arrested at the Battle of the Bulge, they are not brought before a judge, they are not given Miranda warnings. They are held until the war is over or there is some other reason for them to be released. And if these individuals have violated the rules of war, they by history and common sense can be tried by a military commission, without having to do so promptly or on the schedule according to the procedures that the Defense Department feels are legitimate.

So I think the presumption needs to be that persons coming from al Qaeda or other terrorist organizations should be held in military custody; and if at some point it is decided it might be better to try them in civilian courts, the courts have approved that process.

Also, we have had some situations in which individuals are making phone calls in my State indicating that Federal grant money is available, that you can apply for it if you send some group money. It appears to be a fraud scheme, and I would like to talk to you about that.

Thank you, Mr. Chairman. I appreciate you having the FBI Director. We all admire him and admire the FBI, and we look forward to working together to make it better.

Chairman LEAHY. Thank you.

Robert Mueller became the sixth Director of the Federal Bureau of Investigation on September 4, 2001. He had, tragically and horribly, a baptism of fire just a few days later on 9/11. But prior to that, he was U.S. Attorney for the Northern District of California. We have at least two former U.S. Attorneys on this Committee—Senator Sessions and Senator Whitehouse.

The Director began his career at the Justice Department by working for 12 years in the U.S. Attorney's Office of the Northern District of California, chief of that office's Criminal Division, Assistant U.S. Attorney in Boston, and later as the Assistant Attorney General in charge of the Department's Criminal Division. He has his undergraduate degree from Princeton, master's degree from New York University, served in the Marines for 3 years in Vietnam, and then earned his law degree from the University of Virginia Law School.

Director Mueller, the floor is yours.

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

Mr. MUELLER. Let me start by thanking you. Good morning Chairman Leahy, Ranking Member Sessions and Members of the Committee. Thank you for the opportunity to appear before the Committee today. I am extraordinarily proud of the work that our people do.

I also suppose I should thank you for making the hearing interesting this morning. Also, I want to thank Ranking Member Sessions for holding this hearing as well.

Since the Committee's last oversight hearing, the FBI has faced an extraordinary range of national security and criminal threats. These threats underscore the complexity and the breadth of the FBI's mission to protect the Nation in a post-9/11 world. Let me highlight, if I could, a few examples for you this morning.

Over the past year, al Qaeda and its affiliates remain committed to conducting attacks inside the United States as well as against our military and against civilians overseas.

Last September, the FBI disrupted the al Qaeda plot of Najibullah Zazi and others who were planning to attack the New York subway system.

In December, Umar Farouk Abdulmutallab attempted to bomb Northwest Airlines Flight 253 on Christmas Day, an attack directed by al Qaeda in the Arabian Peninsula.

And in May of this year, Faisal Shahzad attempted to detonate a car bomb in Times Square, an attack linked to support from TTP.

And earlier this month, al-Shabaab took credit for detonating two bombs in the Uganda capital of Kampala, killing more than 70 people, including an American.

Homegrown and "lone wolf" extremists also continue to pose a serious threat, as we saw with the attempted bombings of an office tower in Dallas and a Federal building in Springfield.

Combating threats like these requires the FBI to continue improving our intelligence and our investigative efforts, as well as working closely with our intelligence and law enforcement partners, both here and abroad.

The counterintelligence threat to the United States continues to persist, as we saw with the recent arrest of a network of Russian spies. Foreign adversaries, however, do not rely exclusively on such traditional agent networks. They increasingly employ non-traditional collectors—such as students, visiting scientists, business-

men—as well as cyber-based tools to target and penetrate United States institutions.

Turning to the cyber threat, the cyber threat cuts across our national security and criminal programs. To date, terrorists have not yet used the Internet to launch a full-scale cyber attack, but al Qaeda and its affiliates have created a potent online presence. Extremists are not limiting their use of the Internet to recruitment; they are also using it to incite terrorism.

The cyber threats also target Internet businesses, as we saw with the Google intrusion earlier this year. Internet fraud and identity theft remain a growing problem, as the Internet Crime Complaint Center, IC3, reported a 22-percent increase in complaints this year, with more than 330,000 involving more than $550 million in losses.

The Internet has also become a platform for the theft of intellectual property around the world. Last week, a 2-year joint investigation by FBI, Spanish, and Slovenian authorities led to the arrest of individuals responsible for the creation of the Mariposa botnet, a vast network of more than 8 million remote-controlled computers worldwide. Using a computer virus known as the butterfly bot, criminals stole credit card and bank card information and launched denial-of-service attacks. In the last 2 years, the software used to create the Mariposa botnet was sold to hundreds of other criminals, making it one of the most notorious in the world.

These cyber intrusions, thefts, and frauds undermine the integrity of the Internet and the businesses that they rely on. They also threaten the privacy and pocketbooks of all who use the Internet. I should also mention that finding and punishing those who use the Internet to conduct sexual exploitation always remains among our highest priorities.

Let me spend a moment discussing our efforts against financial crimes. Over the past year, the impact of large-scale financial crimes has grown. In the wake of the financial crisis, the FBI continues to uncover major frauds in the thousands of cases we have under investigation, cases such as the Petters $3.9 billion in Minnesota yielded convictions and stiff sentences for top-level executives. In June, the former chairman of a securities firm was charged with a $1.9 billion fraud that contributed to the failure of Colonial Bank. And this month, the former CEO of Capitol Investments was charged in an $880 million Ponzi scheme.

The focus on health care fraud is no less important. As, Mr. Chairman, you pointed out, 2 weeks ago the Medicare strike forces in Miami, Baton Rouge, Brooklyn, Houston, and Detroit announced charges against 94 individuals for more than $251 million in false claims to Federal health care programs. These fraud schemes continue to plague the health care system, including fraudulent billing for home health care, durable medical equipment, and HIV infusion treatments. The number of pending FBI health care fraud investigations has grown steadily and now stands at more than 2,500 cases.

Let me turn for a moment to information technology in the Bureau, a subject to which you alluded.

The FBI has continued to improve and upgrade our information technology. In the past 18 months, the FBI has rebuilt many of our

computer networking systems, deploying the next-generation network to over 800 locations worldwide and providing 45 times greater backbone bandwidth.

The FBI is also replacing our computer work stations with the next-generation workplace which will provide state-of-the-art voice over Internet, desktop videoconferencing, and Web collaboration tools for every one of our FBI users. And the FBI has now deployed more than 26,000 BlackBerrys to its workforce, including recent upgrades that allow direct access to databases like NCIC.

Turning to Sentinel, starting this week the FBI is deploying phase two to all of our offices across the country. Phase two enhances Sentinel's capabilities for the thousands of FBI employees and supervisors who already use it each day. As you pointed out, this last spring we issued a partial stop-work order on phases three and four in order to ensure that phase two was completed successfully. Given the delays associated with the completion of phase two, we are examining ways to reduce costs and limit our reliance on contractors to keep the project within its budget. Currently the FBI is consulting with industry experts to evaluate our plan to finish Sentinel.

In closing, as the Committee knows, the FBI faces a new budget climate in the coming year. Along with all other agencies, we are being asked to reduce costs and eliminate redundancies wherever possible, which we will make every effort so to do.

To conclude, I appreciate the opportunity to discuss the FBI's recent work responding to the complex and the far-ranging threats we face today. I also want to thank the Committee for your continued support of the FBI in its mission, and, of course, I would be happy to answer any questions that you might have.

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

Chairman LEAHY. Thank you very much, and I appreciate that.

The Washington Post ran a series last week on the extraordinary growth of the intelligence community since September 11, 2001, and the terrorist attacks. But they also highlighted the increased reliance on private contractors. I talked with you briefly about this yesterday, but as you know, I am very concerned about sensitive national security work being done by for-profit companies rather than being done by public officials. And I was worried about all the overlapping use of private contractors that article or series of articles came up with.

Now, aside from foreign language translators and information technology workers, how do the intelligence components of the FBI use contractors? How much of your intelligence work is comprised of contractors? I should note that series showed that you have a lot less contracting companies in the National Security Agency or the Department of Homeland Security or the Department of Defense. Please go ahead, sir.

Mr. MUELLER. We, of course, use contractors. We for several years now have undertaken to reduce our reliance on contractors. One of the areas that you mentioned is the IT arena, for instance. We have built up our in-house capabilities, which will enable us, I believe, to do some of the work that traditionally has been done by contractors.

But to give you an example of the use of contractors, we have a Weapons of Mass Destruction—WMD—Division. There are periods where we need particular expertise to gain knowledge in an area in which someone outside will have the expertise and we do not have the expertise in place. So we will bring a contractor on for a period of time, whether it be in the nuclear arena or the biological arena or the chemical arena, for a period of time to help us establish a program. That is an example in, I guess you would call it, the intelligence arena where we use contractors.

But we are sensitive to the fact that there are discrete areas where, as you pointed out, whether it is language translations, that contractors have a role. There are other areas where the work should be done in-house, and we are scrutinizing that.

Chairman LEAHY. Given your druthers, would you prefer in-house to contractors?

Mr. MUELLER. Given my druthers, I would prefer in-house, both for the savings as well as developing the core capabilities.

Chairman LEAHY. The press reported this morning that the Inspector General of the Department of Justice is investigating whether FBI agents across the Nation cheated on a mandatory test on the FBI's Domestic Investigations and Operations Guidelines, the DIOG. This has been a source of concern. I along with a number of other Senators on this Committee had to really wrestle with former Attorney General Mukasey for months just to obtain a copy of this. Once we read it, many expressed fear that this broad authorization of domestic investigative techniques had the potential to encourage racial profiling. The FBI assured the Congress that the test that agents take and the content of DIOG would ensure that agents are fully trained on not only the scope but the limitations of the FBI's authority.

Now, we learned last year that a small number of agents were accused of cheating on the test. That is what I was told. I was amazed when I went online this morning to find from press accounts that cheating was reportedly more widespread.

What is the scope of the investigation? How many agents are involved? What steps have you taken to make sure this does not happen again?

Mr. MUELLER. Let me start, if I could, because your question addresses a number of issues that were raised.

First of all, in terms of the guidelines, the new Attorney General guidelines, the point that should be made at the outset is that we do not, the FBI does not target persons or groups based on race, ethnicity, or religion. That is at the heart of those guidelines. And that is what we teach each of our personnel.

After the guidelines were signed into place by the Attorney General, we undertook a substantial education program for our agents, having developed the DIOG, and all of our agents and much of our other personnel went through that training, more than 16 hours of training.

There was a test given a year ago. It was an open-book test. The parameters were that you could use what materials you wanted to, it was open book, but you should not get help from another person.

Early on, we in the Bureau had allegations that those procedures were not followed in particular instances. We investigated those instances and took appropriate action.

The Inspector General has taken over that investigation and has indicated that there are additional personnel that did not abide by those procedures. We do not have all the specifics, and we are expecting a letter from the IG pointing out other occasions where there were abuses and the procedures were not followed with recommendations, and we will follow those recommendations.

In the meantime, however, it is quite obviously my concern that all of our personnel understand the parameters in which we are to work. I am confident that the training and the testing and the continuous training we have has put our workplace—or our people in a position to fully know and understand the opportunities but also the limitations of what we can do. There are various levels of review.

I will tell you one other statistic. After the training was completed and the test taken, the incidence of errors in the paperwork was reduced by 80 percent. And so I do believe that our workforce absolutely understands what can be investigated, how it must be investigated, what predication is necessary for a particular investigation in this day and age.

Chairman LEAHY. How many agents were involved in cheating on the test?

Mr. MUELLER. At this point I do not know. I do not have the report from the IG.

Chairman LEAHY. Do you have any idea?

Mr. MUELLER. I have got a general idea, but I do not know how many, and I am not certain the IG knows how many either. He has pointed out instances orally to me where there may be persons in a particular office where it was widespread, and it may be attributable to a lack of understanding and confusion about the procedures.

Chairman LEAHY. We will be asking the IG these questions.

I do have one last one. A year from now, when we have a hearing, what will you be able to tell us about Sentinel? And where will we be with Sentinel then? I mean, you have wrestled with this. We have wrestled with this whole question of the computer system of the FBI. We have seen fits and starts. Where will we be a year from now?

Mr. MUELLER. Well, a year from now we certainly, I believe, will have successfully completed phase two. We ought to complete that at the latest this fall. Phase two is the heart of the system. It puts on agents' desktops a case management system. My expectation is that—from what I hear from around the country, it is work successfully. When I issued the initial partial stop order, it was because I was not satisfied that we had eliminated all of the coding errors that may be there, and I was not satisfied as to the scalability.

After engaging in three pilot projects that were successfull, we ran that out this week, and the heart of the system is in place.

The additional capabilities that we were seeking in phase three and four, we are looking to determine how best to go forward and obtain those capabilities. We have employed experts from outside

the Bureau to look at it, and my hope and expectation is that we will be able to deploy many if not all of those capabilities given two factors: one, the enhancement in technology since this contract was initially issued 5 years ago; and, second, our ability to use our own staff for much of the development here on in, which goes to the building up of that IT staff and less reliance on contractors. We have built up our own IT staff. We benefit from technology advances. We ought to be able to make a substantial savings on phases three and four.

Chairman LEAHY. Please keep us posted on that because I think there has been bipartisan concern on this, and it is justifiable.

Mr. MUELLER. I understand.

Chairman LEAHY. Senator Sessions.

Senator SESSIONS. Mr. Chairman, I would yield my time to Senator Grassley, who works very hard in this Congress to protect the Treasury of the United States, and I know he has some questions to ask, so I would yield to him at this time.

Senator GRASSLEY. I am going to continue where the Chairman just left off on Sentinel. In March, I wrote to you after learning the FBI issued a stop-work order to the prime contractor, Lockheed Martin. The reply I received indicated that this was temporary and would help assure delivery of phase two by this summer.

Just last week, I wrote you a letter here again about the new stop-work order. I have yet to receive a response, but the FBI issued a press release saying phase two was not anticipated, as you just said, by—well, at least the press release said by the fall of 2010. I understand that phase two was released to the field just this week, but that may not be final until fall.

I find all of this uncertainty in a major procurement very concerning. We have not been getting answers from the FBI about the projected cost or timeline on finishing the program. I am concerned that the uncertainty is a signal that the FBI will be unsuccessful in finishing Sentinel. I know you just said the opposite to the Chairman. This project was scheduled to be finished December 2009 at a cost of no more than $451 million. In a lot of correspondences we have had on this issue, the word keeps popping up about we are negotiating, we are negotiating, we are negotiating. And you wonder how much negotiation goes on when $451 million is involved.

The timeline is a bust. The Inspector General noted that the FBI does not have a current schedule or cost estimate for completing the project. I asked for these estimates in March, and the FBI said it was negotiating with Lockheed Martin. There was no indication when we would get these projections. That is unacceptable because the American taxpayers deserve answers given the ballooning Federal deficit and endless delays in the program.

Based upon negotiations with Lockheed Martin, how much longer will it take to complete the Sentinel system? When will it be finished? In May, the Washington Post reported that you believe Sentinel will be done be 2011. Do you still believe that that date is accurate?

Mr. MUELLER. You covered a lot there, Senator. If I might, I will start off by saying, as you pointed out, when I issued the partial stop-work order—I think it was in March—I indicated at that point

in time that we wanted to do pilots in order to assure the feasibility, viability, and scalability of the system that upon success of those pilots that phase two would be deployed this summer. And as I said before and as I told you what happened, it is being deployed, and it should be deployed by—certainly the deployment should be finished by the end of this summer.

We broke this project up into phases so we could look at each phase, learn lessons from each phase, so that we would not be bound by one overarching contract but could go and accept the project piecemeal. I am actually pleased that the heart of the program phase two is now on agents' desks and a case management system is there.

Augmenting that will be additional forms and additional capabilities, we have to look at both the budget and the timeframe down the road and determine how much of that work can or should be done by the contractors, how much of that work can and should be done by ourselves, given the new technology. And as we finish phase two, that will be what we are looking at in the next 3 months.

So I cannot at this juncture right now give you hard figures, but we have endeavored both for you in this Committee and other committees to keep you apprised of everything that happens in the course of our developing this software package.

Senator GRASSLEY. So you are saying you cannot give us a date, if it will be done by 2011?

Mr. MUELLER. Not until we have additional information based on what we have found to be both problems and successes in phase two. It is exactly what we did when phase one was completed in, I think it was, 2007. We went back, looked at the areas in which we were successful and looked at those areas where we failed and adjusted. We will do that again.

Senator GRASSLEY. Has Lockheed Martin provided a cost estimate to finish Sentinel? How much more will the taxpayers have to pay? Is it hundreds of millions of dollars, tens of millions of dollars? Can you tell us if the cost is going to exceed $1 billion?

Mr. MUELLER. Certainly it would not exceed $1 billion, but I can tell you, as you pointed out, there was an overarching budget for this project. We hope to stay within that budget. There are ongoing negotiations, but I am mindful of the necessity of maximizing the products that we get and minimizing the cost to the taxpayer, which is why, as I say, we are looking at alternative capabilities and with less reliance on contractors who can prove to be more expensive than if you could do it yourself in-house.

Senator GRASSLEY. In March, the FBI said it spent over $25 million on phase three, which is now indefinitely delayed. Is that money lost and gone forever? Or will the FBI recoup those monies from the contractor?

Mr. MUELLER. That will go into our evaluation of where we go with phases three and four. As I pointed out before, we engaged in an incremental development process so that we could adjust throughout the contract.

One of the, I think, striking differences from what we had not accomplished before is the fact that we have a case management system that is now working for the Bureau.

Senator GRASSLEY. Does the FBI plan to continue working with Lockheed Martin? Or are you going to consider hiring another contractor to complete phase three and four? And while you are answering that, does the FBI believe that it has gotten a good deal from the money on Sentinel so far?

Mr. MUELLER. We have a case management system through the Sentinel development process that we never had before. With regard to the extent to which we continue to work with Lockheed Martin, I do believe we will continue to work with Lockheed Martin, but we still have to iron out exactly what the roles will be and the amount of money that we want to expend through the contractor and the amount of money we want to expend in-house to continue development.

Senator GRASSLEY. The FBI has issued over 39 contract modifications. However, that number is deceptive as phase two had 160 change orders rolled inside of those modifications. Does the FBI know what it wants? Or is the FBI passing up a good system in order to just try to have a perfect one?

Mr. MUELLER. I think what you point to is an issue everyone who develops software packages has to wrestle with. Over a 5-year period, our mission has changed to a certain extent. Our necessities have changed. Things like the Attorney General's guidelines have changed. Our processes have changed, which requires us—if you lock in the requirements in 2004 in order to issue the contract, things are going to change between 2004 and 2010. And while there have been modifications, I think they are relatively minor modifications, and not the principal contributor to whatever delays there have been.

But you have to take that into stride, and you have to have a balance, on the one hand, of making the system work for your people, and on the other hand, staying within the requirements and the cost estimates and time estimates that you contracted to 4 or 5 years ago. And that is what we wrestle with.

Chairman LEAHY. Thank you.

Senator Kohl, then Senator Sessions.

Senator KOHL. Director Mueller, last week's Washington Post series on the growth of our intelligence efforts highlighted the tendency of both Congress and intelligence agencies to respond to terrorist threats by expanding programs and hiring more analysts. Since 9/11, the FBI has been expanding to meet its counterintelligence mission within the United States. However, we all know that bigger is not always better. Many intelligence officials seem to agree. In that article, Defense Secretary Gates said that he plans to review the Department of Defense for programs in terms of waste. Similarly, CIA Director Leon Panetta said that he is looking at ways to reduce the CIA's spending, describing the current level as "unsustainable."

Has the FBI done a thorough review for waste overlap and redundancy? Or do you have plans to do so? And how do you decide when more resources are needed or when it may be appropriate to scale back?

Mr. MUELLER. We have for a couple of years now looked at the contractor's program from a variety of perspectives: first of all, knowing and having a handle on all the contractors you have in an

organization. And I think we have a very good handle on the number of contractors that we have and the jobs that they are performing.

We have in certain areas, particularly in areas like counterterrorism, sought to reduce the number of contractors, and we have recently adopted additional programs to give incentives to our leaders within the Bureau to reduce the number of contractors.

I will tell you that when it comes to the intelligence work that we do, it is performed generally by agents who I would call the collectors as well as analysts. We have hired since 2001 over 2,000 analysts in-house, not relying on contractors but our own in-house analysts that have come with substantial educational backgrounds and many with experience in other agencies, to address the need to bring on people in the intelligence arena.

That being said, there is still more that we can do, and we are looking at each of the job series and providing incentives to managers to reduce the number of contractors, to minimize them, and to eliminate whatever overlap there may be.

Senator KOHL. The entire intelligence system has expanded rapidly, as you know. By the end of 2001, 24 new organizations had been created, and dozens more are added each and every year. Over the past 9 years, existing intelligence organizations and agencies have more than doubled in size.

Director Mueller, you became the FBI Director just before 9/11. You have seen firsthand the massive expansion of our counterterrorism efforts since it began. In your view, should there be more than an agency-by-agency review? Should there be a large-scale comprehensive review of this growth since 9/11 to assess its effectiveness?

Mr. MUELLER. I am familiar with the Washington Post articles, and I, of course, would participate in and would be open to any suggestions from any entity that provided a review to the intelligence community. I am not certain it would affect us dramatically. We have a distinct and I think very important role to play in addressing terrorism within the United States. And I do believe that we have resources adequate to that task now, but we have had to take those resources from other priorities within the organization.

I am probably not the best person to ask as to whether or not there should be an overarching review. I am comfortable with what we have done, and I would leave the decision as to whether there ought to be an overarching review to others who are more familiar with the work of areas of the intelligence community with which I am not familiar.

Senator KOHL. With respect to the possibility of an overall review would you support an independent commission? Or should the review come from within the intelligence community?

Mr. MUELLER. I am not certain that there is a necessity for a new commission. To the extent that there needs to be elimination of overlap, a coordination of response, I think we do a pretty darn good job now in the terrorism arena. That does not mean that there are not areas that we could look at, but I do believe that the Office of the Director of National Intelligence has that as one of its mandates, and that is to look for areas of overlap and address those

areas. In my experience, that has happened in the past, and my expectation is it will happen in the future.

Senator KOHL. Director Mueller, the Justice Department Inspector General released a report in June concluding that none of the agencies within the Department, with the exception of the FBI, have operational plans in place to respond to a terrorist attack involving a weapon of mass destruction. The Inspector General described the rest of the Justice Department as "uncoordinated and fragmented" and finding that the Department's critical incident response plan has not been updated since 1996, and it is completely unprepared to coordinate Federal law enforcement response activities if called upon to ensure the public safety.

Director Mueller, we are pleased that the FBI has taken adequate steps to respond to a WMD attack. Are you working with other components of the Justice Department to ensure that they, too, become adequately prepared?

Mr. MUELLER. Well, the credit for all of that goes to our WMD Division and the leadership there, and, of course, our leadership has offered to, and I believe will, assist other components of the Department to learn from the lessons that we have had to learn ourselves.

Senator KOHL. Are you working with these other departments?

Mr. MUELLER. I would have to get back to you specifically on what we are doing. I know we are working with the Deputy Attorney General's office to provide our expertise to the other agencies, and how we are doing that and what particular methods are used, I am not familiar. I have to get back to you on that.

Senator KOHL. Director Mueller, as you know, the threat of fraud facing seniors is growing and evolving. Criminals are expanding their targeting techniques from traditional telephone calls and mass mailings to online scams, and seniors continue to be scammed out of their lifetime savings. According to a 2009 report by the MetLife Mature Market Institute, the annual financial loss by victims of senior financial abuse is estimated to be at least $2.6 billion.

Senator Gillibrand and I have introduced a bill, the Senior Financial Empowerment Act, S. 3494, that would require the FTC to partner with the FBI to disseminate information about mail, telemarketing, and Internet fraud targeting seniors to seniors and their families or caregivers, local law enforcement, and advocacy organizations that work to protect seniors from fraud.

Are you familiar with the legislation? And if you are, do you support it?

Mr. MUELLER. I am generally familiar with the fact of the legislation. I cannot speak for—the Department of Justice has to issue opinion letters and the like, but I do believe for ourselves, even without the legislation, it is important for us, whenever we come across a particular fraudulent scheme that addresses the elderly, to not only address it by investigating, indicting, and convicting the persons responsible for that scheme, but alerting others around the country, other task forces about that scheme. And we have a regular procession of intelligence reports that we push out that alert others in the community, whether it be the health care community or the law enforcement community, to what we have found in one

area of the country to alert others in other areas of the country to accomplish that. And to the extent that there is legislation that supports that, we would be supportive.

Senator KOHL. I would appreciate it if you would take a look at our legislation and let me know if I could have your support on it.

Mr. MUELLER. Yes, sir.

Senator KOHL. Thank you so much.

Senator Sessions, we now call upon you.

Senator SESSIONS. Thank you, Senator Kohl.

Director Mueller, to follow up on the discussion we have had previously concerning how terrorists should be treated when they are arrested in the United States, you responded to Senator Hatch that, pursuant to HSPD–5—what is that, HSPD–5? Is that a——

Mr. MUELLER. It is a directive from the President that gives us certain authorities.

Senator SESSIONS. All right. The Attorney General—I am quoting here from your answer—"has the lead responsibility for terrorism acts committed in the United States."

First let me just say that is a bit odd if we were attacked by an army enemy. I do not think that would be the case.

But continuing, "Consistent with that responsibility, the FBI will respond to the scene of any such attempted terrorist attack and will conduct an appropriate investigation in compliance with the Attorney General's guidelines for domestic FBI operations." And then you say, "The FBI has no legal authority to proceed against a terrorism suspect who is arrested within the United States in any venue other than an Article III court."

That is civilian, normal Federal court.

"There have been only two instances in 2001 in which civilians were arrested that were placed in military custody for some period of time."

You do not mean to say by that that you could not participate in the arrest and if it is clear that the individual is a terrorist connected to al Qaeda, that they cannot be turned over to the military for prosecution, are you?

Mr. MUELLER. No, I am not. I do not mean to say that.

Senator SESSIONS. If you are involved in that arrest of this terrorist, can you not proceed with the assumption they will be turned over? Or do you have to follow all the rules and regulations that the FBI must follow when they arrest a normal American criminal?

Mr. MUELLER. Well, our authority is derived, I believe, from Title 18 and others that authorize us to make arrests pursuant to certain criminal statutes, and it is somewhat limited in that regard. That does not mean that the President cannot direct that we turn an individual over to a military commission and military court, and that has happened in the past. But in——

Senator SESSIONS. Does it take Presidential authority to make that decision?

Mr. MUELLER. Pardon me?

Senator SESSIONS. Does the President himself have to make that decision? Can't he set a policy or regulation that would allow that decision to be made?

Mr. MUELLER. That went a little bit beyond my constitutional depth, and that is the type of question in my mind that should be

answered by the Office of Legal Counsel. But for us, we can do the arrest. We do it pursuant to certain authorities. But then a determination can be made by the President that it go elsewhere.

Senator SESSIONS. Well, normally you would give Miranda in less than 50 minutes—you waited 50 minutes, and I hope and believe you probably had a basis to wait that long, but it is pushing the limit. Under normal situations the Miranda has to be given immediately if you ask questions of the defendant once they are placed into custody.

So I am worried about this whole process. It is not working logically to me, and some say, well, they could confess after being given Miranda and they could plea bargain or something if they are taken through the civilian courts. But there is much more ability for the U.S. Government in dealing with an unlawful enemy combatant, a terrorist attacking the United States, it seems to me, if that individual is placed into military custody where they belong if they are an enemy combatant. Aren't I correct about that?

Mr. MUELLER. We have had this discussion, I know, Senator, and I am every bit as interested in and concerned that we get intelligence as soon as possible with regard to other potential attacks. And even in the case of Abdulmutallab, who came into Detroit, utilizing the Quarles exception, he was interviewed for a period of time by our agents without Miranda warnings.

In each of the instances that have reached the newspapers recently, there has been a variety of positions taken early on as whether to Mirandize or not. In each case, we have gotten the intelligence we have needed. So——

Senator SESSIONS. I do not think—that is not impressive to me. I am not worried about what has happened anecdotally in some individual case. Clearly the policy, in my judgment, would be better if you took the other view and they were presumptively held by military custody. And it does appear to me that Homeland Security Directive HSPD–5, signed in 2003 assigned the Attorney General the lead responsibility to investigate this, and that you are following Department of Justice policy in this regard. If that policy is to be changed, you do not have the authority to do that. Is that correct? That would have to be done by the President or the Attorney General?

Mr. MUELLER. We would follow the policies as set by the Attorney General pursuant to the policies, legal policies set by the President. We do believe the President has the authority to make the decision as to where an individual will be tried.

Senator SESSIONS. So that is where the responsibility lies, with the President of the United States, and they are persisting in an unwise policy, in my view, that cannot be justified. But that is another matter. We will continue to pursue that.

Let me ask you about fraud filings. In 2003, bank embezzlement cases under the FBI enforcement were 395 case filings; in 2008, 186. Bank institutional embezzlement cases were 44 in 2003, 37 in 2008. Financial institution fraud was 916 in 2003, 524 in 2008. SEC-related fraud was 118 in 2003, 66 in 2008. Bankruptcy fraud, which is Federal court, nobody else investigates bankruptcy fraud except the FBI—perhaps the Secret Service on occasion—was 92

only in 2003 and dropped to 52 in 2008. You and I have talked about bankruptcy fraud cases before.

It seems to me that these represent a very, very serious decline in fraud enforcement at a time we have had major problems with banks failing, allegations of misconduct and fraud out there. What is happening to cause such a decline in prosecutions?

Mr. MUELLER. At the outset, I would have to look at those figures. Some of them do not seem accurate to me. But putting that aside, that is part of the picture.

After September 11th, we had to prioritize. One of the areas we prioritized is the focus on larger white-collar criminal cases. We could not take the bank teller cases. We could not take the smaller embezzlement cases. And the numbers inevitably went down as a result.

As you have seen and all of us have been through in the last 2 to 3 years, we have a mortgage fraud crisis, we have a securities fraud crisis, and we have a corporate fraud crisis. We have focused on those cases where there are multi-million dollars at stake, where the investors have lost millions if not billions of dollars, and that has been the focus.

Inevitably when you focus on the larger cases, the smaller cases will not be there to give you the numbers you had before. But I am comfortable that we prioritized appropriately.

Senator SESSIONS. Well, I am not comfortable with the decline in prosecutions, so I am going to look to find out more about that. I have heard that spin from FBI Directors and the Department of Justice for 30 years—25 at least—that we are working bigger cases, that is why the numbers are down. Haven't you heard that?

Mr. MUELLER. Well, we have both heard it, but I can tell you at this time it is true. And I will tell you that—you look at the cases, you look at the indictments, you look at the Petters investigation that was successfully prosecuted in Minneapolis, where something in excess of $1 billion was lost to the investors. That is the type of case we are bringing, and successfully bringing.

Senator SESSIONS. Thank you, Mr. Chairman.

Chairman LEAHY. And the quarter of a billion dollar one that I mentioned earlier.

Senator Cardin.

Senator CARDIN. Well, thank you, Mr. Chairman.

Director Mueller, once again welcome to our Committee, and thank you very much for your service to our country. We very much appreciate that.

I want to follow up first on two questions that were asked, one by Senator Sessions and one by Senator Kohl. Senator Sessions' question to you, I want to make sure we get the full answer, because I believe you were saying that in regards to someone who is apprehended, you are confident that the current policy allows you to interrogate to get—to do your best job to get information to protect the safety of the people of this Nation, whether it is someone who is doing terrorist activities or criminal activities, that there is enough flexibility in this policy in regards to the exceptions under the Miranda rights, or the other options that are available in evidence to bring criminal matters or go to military tribunals, that the

current policy allows you to question to get information that you believe is critically important to the safety of Americans.

Mr. MUELLER. I do believe that we effectively handle terrorism cases in the United States, both from the perspective of investigation and at the appropriate time, after we have developed maximum intelligence, arresting and then participating in the prosecution of individuals. I also believe that we do an effective job of interrogating, questioning individuals once they are detained here in the United States. In those circumstances where it is appropriate because the individual has information perhaps relating to other terrorist attacks to take advantage of the Quarles exception and do extensive questioning on that particular issue before we Mirandize an individual, and that at the appropriate time Mirandize that individual so that whatever is said afterwards can then be used in the prosecution.

Senator CARDIN. I thank you for that answer, and, of course, the Miranda rights concern information obtained. You can obtain information from other sources. There may have been statements made before. There may have been other evidence available to deal with criminal convictions.

Mr. MUELLER. Correct.

Senator CARDIN. Following up on Senator Kohl's point dealing with the IG's report—which was very complimentary of the FBI as it relates to preparations against attacks with weapons of mass destruction. Next week, the Subcommittee that I chair, the Subcommittee on Terrorism and Homeland Security, is going to hold a hearing on this subject. Senator Kyl has asked us to do this. He is the Ranking Republican Member of this Subcommittee. And I would like, if you could—it may require you to get back to us, but you commented very briefly about what lessons you have learned that could be helpful to other agencies under Department of Justice.

It looks like that you have taken this issue very seriously. You have designated a key person for a response, and you are prepared to do everything you can to prevent an attack, but also to be prepared to deal with threats that may be here.

Now, working in the Nation's capital, we are the epicenter of concern about those types of attacks. I represent the State of Maryland. The counties that are close by are almost in the bull's-eye area. So we are very interested in making sure that the lessons that you have learned in the FBI are not only shared but implemented by other agencies in the Department of Justice to make sure we are as prepared as we can be against this threat against America.

Mr. MUELLER. We have not forgotten the lessons of the anthrax attacks many years ago and have to assume—not that there is any threat currently, but that we have to be prepared to address it, not just in the Nation's capital but around the country.

And so our program required the establishment of a particular division that was dedicated to this in all of its various aspects—nuclear, biological, radiological—but also around the country training individuals and additional persons to both investigate and respond to such attacks.

So our program is not just headquarters-centric. It is throughout the United States, including, quite obviously, in Maryland. And we have capably trained individuals who are responsible for both the investigation and responses in every one of our 56 field offices around the country. It is those how we have organized any lessons that we have learned in terms of how you best maximize that organization that we are hopefully passing on to others who have certain responsibilities in the field as well.

Senator CARDIN. Well, we thank you for that, and we look forward to working with you in our Subcommittee as we try to get even better at preparation for these types of threats. So thank you on that.

During our discussions on the hate crimes legislation, we talked a great deal about the Federal Government working with local governments in cooperation. Local governments today are having a very difficult time with their budgets. I am sure you are aware of that, and we have seen that locally in our State where there is concern as to whether there are the resources that go after different types of criminal activities. Gang activity seems to be on the rise in some parts of my State and in other States around the Nation.

Can you just share with us what steps you are taking to work with local governments to deal with the concerns that the current economic crisis and budget problems are having on effective law enforcement?

Mr. MUELLER. I have two areas in which we attempt to address this. First, in the wake of the legislation, training, providing training programs to State and local law enforcement about what the Federal law is and how we would work with them to investigate hate crimes; sensitizing them to law, and we have done that around the country in many jurisdictions.

Second, one of the deficiencies is the reporting of hate crimes, and we encourage throughout the country to our various field offices the reporting of hate crimes so that we have an accurate view of what is happening across the country. Those are two areas in which we have followed up.

Senator CARDIN. Well, thank you. The last point, I just want to compliment you. In your written statement, you deal with the Civil Rights Unit's work, and you bring up the Danziger Bridge episode, which I think was the right steps taken by the FBI. I just would encourage you in regards to the civil rights issues to keep a focus on this. We are concerned, again, about the rise of specific cases that are being brought. The trafficking issue that you mention in your report, we have seen some increased activity in trafficking, that I would just encourage you to give the highest attention of your agency.

Mr. MUELLER. Yes, sir.

Senator CARDIN. Thank you.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Senator Hatch.

Senator HATCH. Thank you, Mr. Chairman.

Welcome. Good to see you again, Mr. Director. We appreciate the work that you do, and all of you at the FBI I have been very appre-

ciative of over all these years of watching what you do, and you do a great job.

Let me turn your attention to criminal gangs. Specifically, I want to discuss MS–13. Now, the FBI has previously described MS–13 as the most dangerous gang in America. MS–13 traces its origin to El Salvador. Ultimately they reached Los Angeles and now have an estimated 10,000 members in, I think, at least 33 States. They stockpile and traffic in weapons. They have a business model that brings in revenue through extortion and shakedowns of merchants for "protection fees."

A Mexican drug-trafficking organization identified as the Sinaloa cartel has contracted out to MS–13 for a wide variety of illegal activities. Now, that activity includes drug smuggling and illegal alien smuggling. Recently Arizona State law enforcement sources believe that an MS–13 member might have murdered Arizona rancher Robert Krentz. MS–13 is the example of why securing the border, combined with a tough and coordinated law enforcement approach is badly needed.

In 2006, the only documented Federal informant to provide insight into this organization, Brenda Paz, was brutally murdered by MS–13 in Virginia. One of her MS–13 attackers had previously been deported after he was arrested for a stabbing that he committed in Florida.

For several years now, I have been working with the distinguished Senator from California, Senator Feinstein, to get comprehensive and tough gang legislation passed into law, anti-gang legislation. This enforcement legislation includes prevention and strict penalties to dismantle not only MS–13 but any criminal gang. Now, I am well aware that the FBI has a national task force focused on MS–13.

Now, to the extent possible, could you give us an update on FBI activities and investigations directed at MS–13?

Mr. MUELLER. Senator, as you rightly and appropriately point out, MS–13, a longstanding gang out of initially Los Angeles, generally El Salvadoran, has spread its tentacles throughout the United States over the last 10 years. We currently have over 190 task forces around the country that address gangs, violent criminal enterprises, with over 2,200 agents that are working this.

More particular to MS–13, we have an entity here at headquarters that monitors it and develops intelligence on that gang. But perhaps more importantly, we have a task force down in El Salvador, individuals working with our El Salvadoran counterparts to address MS–13, because you do find that MS–13 members travel back and forth—not necessarily at will, but very easily—between the United States and El Salvador.

We also have a fingerprint initiative that we have had for a number of years that focuses on MS–13 that we are operating with our counterparts in El Salvador. We also know that there are elements of MS–13 in Guatemala, Honduras, and in Mexico. And our legal attache offices work with our counterparts in each of those countries to share intelligence and coordinate takedowns of the elements of MS–13.

It is one of our highest priorities when we look at criminal enterprises, gangs, and violent crime.

Senator HATCH. Thank you for that summary.

Mr. Director, our Nation's cyber defenses are vulnerable, and action must be taken quickly to address the threats that our networks and critical infrastructure are faced with every day. Last week, President Obama's nominee to be the next Director of National Intelligence, General James Clapper, praised the concept of establishing a national cyber center and a director responsible for organizing the Government's defense against these cyber threats. This cyber director would be modeled after the Director of National Intelligence, and he would coordinate the Government's cyber defense, threat analysis, response coordination, and information sharing.

Like the National Counterterrorism Center, the new cyber center would collocate representatives from across the Government from both law enforcement and the intelligence community. Importantly, this center would not be based in any one department or agency, so it would be in a good position to see across the entire spectrum of Government defensive cyber activities without getting caught up in the various turf battles.

Now, based on your experiences with deconfliction and sharing information within the intelligence community and law enforcement, what benefits do you see from creating a national cyber center and a director position based on these models? And what contributions do you believe the FBI could make to this type of a center, especially with respect to counterintelligence and cyber expertise?

Mr. MUELLER. I do think the concept of a cyber center makes some sense, but I can tell you that I believe the building blocks are already in place for that. The recent establishment of a Cyber Command under the military will, in my mind, bring together a great deal of expertise under Keith Alexander, General Keith Alexander, on the intelligence and the military side of the house. On the domestic side of the house, we already have the National Cyber Investigative Joint Task Force, which is a stand-alone task force with anywhere from 14 to 17 contributing agencies whose sole purpose is to identify particular threats, whether it be a botnet or a denial-of-service attack, and determine the attribution of that particular attack, understanding that it can come from a State, it can come from individuals associated with a State entity, or it can come from an organized crime group, or, last, it could come from that high school student that is living across the street.

The National Cyber Investigative Task Force has been very successful in addressing these threats, bringing together these individuals. Expanding that, that which has already been successful, I think fits into the model that you are suggesting, and I would welcome each of the members and their staff to come and take a tour of that task force and see the type of work that they are doing. I think it will be illuminating. But I do think it is one of those building blocks that is there that can be expanded to fit the role that you suggested.

Senator HATCH. Well, thank you so much, and thanks for your service.

Mr. Chairman, my time is up.

Chairman LEAHY. Thank you very much.

Senator Whitehouse, please go ahead, sir.

Senator WHITEHOUSE. Director, let me join my colleagues in thanking for your service. You have been one of the constants over the years in our national security team and in the Department of Justice team, and it is a pleasure to have you back.

I serve with Senator Hatch on the Intelligence Committee, along with our Chairman who is here, Senator Feinstein, and the issue of cybersecurity is one that is very much at the forefront of the Intelligence Committee's concerns right now. The President's nominee for Director of National Intelligence, General Clapper, was before us the other day for his confirmation hearing, and he indicated in his listing of the major threats that he perceived, No. 1 on his list was cybersecurity, cyber attack. You have described it in your testimony today as an ever increasing wave, and you mentioned that reported cyber offenses have seen a year-to-year increase of 22 percent.

What I would like to ask you about is your take on the extent to which you feel that the reported offenses provide an accurate snapshot of our Nation's vulnerability to cyber attack, and if you could carve out your answer into two separate pieces, I would appreciate it. The first would be where the victim is actually witting that they have been a victim of a cyber attack, but say for competitive business reasons they would rather not report it and have all their competitors pick up the phone to their clients and say, "If you want to come to a more secure brokerage, try us. We are not in the newspapers as the victims of a cyber attack."

The second, particularly in the intellectual property area, is American companies that are not even aware that they are the victims of theft of their intellectual property, that they are being raided without being witting of the fact that often foreign interests are just siphoning out their intellectual property and using it against them for competitive purposes.

In the wake of those two concerns, do you think that the reported offenses are the bulk of our risk, a small subset of it? What is your take on how the reported offenses fit into the larger picture of our cyber vulnerability?

Mr. MUELLER. From my perspective, if you look at IC3 and the types of referrals that are made to IC3, they probably do not include some of the more important, such as the Google intrusion would be an example of it. And what you advert to in terms of the reporting or failure to report is something that has been a problem over the years. I spent some time in Silicon Valley as a prosecutor there. One of the biggest challenges we had is to explain to companies that they need to report it to us in order to assure that others do not face the same fate, whether it be a denial-of-service attack or a botnet attack or what have you, and that we have to operate together.

Not all companies agree to that for the reason that you said. It can reduce the value of the stock tomorrow if it looks like some of their clients' names and data has been put on the Internet.

Every speech I give, I make a point of saying we have got to do this together, you have got to report, and I know there are certain statutes that are being contemplated that would mandate the reporting. And so——

Senator WHITEHOUSE. Do you agree that the underreporting of this particular crime or act of piracy, or whatever you want to call it, act of espionage, is a problem that merits attention?

Mr. MUELLER. Yes. And what they do not know also is there are statutes that allow us to maintain the privacy of their intellectual property when they come to us to identify an attack, and it is partially an issue of education, but also encouragement and giving them an incentive to report in order to up those statistics. And I am not sure that those are reflected in the uptick of statistics that we see from IC3.

When it comes to intellectual property and the theft of intellectual property, it is rampant, and that is an understatement. And we, of course, have to prioritize. We received an additional 31 agents back in 2009 for this particular area. We have deployed them to four cities where we think they can make a maximum contribution. But we look for the larger cases or the more important cases, an example being——

Senator WHITEHOUSE. Let me interrupt you just for 1 second for a question for the record. I do not want to take your time on it right now, but I would like to see a deployment diagram of where your resources are deployed and to what purposes in the cyber protection area, if I may have that as a written question for the record. Thank you.

Mr. MUELLER. Happy to provide that.

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

Mr. MUELLER. The only other point I was going to make is we do have to prioritize. For instance, when it comes to health and safety, if there are counterfeit airplane or aircraft parts out there, that is something that has the additional element of being a threat to the public that makes it the priority.

Senator WHITEHOUSE. Yes. Well, "rampant" as an understatement I think is a good way to describe it, and I appreciate that you described it that way.

Let me turn to the question of civil remedies in this area. The Microsoft company recently did a very effective civil action against the Waledac botnet and was able to, through the service providers, interrupt the command-and-control functions of the botnet and more or less shut it down.

In the event that the Department of Justice determines that a civil remedy, particularly where attribution might be a problem, is a more effective way of limiting the country's exposure than a criminal prosecution, is the FBI, nevertheless, prepared to dedicate agents and resources to supporting a civil investigation and potentially civil orders that would eliminate access for miscreants to our cyber network?

Mr. MUELLER. Well, I would tentatively say yes, depending on the case and the circumstances. I mean, there is so much work out there on the criminal arena that has to be done that we would focus, quite obviously, on those cases where we can put somebody in jail for that activity so they cannot do it again.

Senator WHITEHOUSE. But you do not feel you need new authorities? It is a priority question.

Mr. MUELLER. No, we would not need new authorities.

Senator WHITEHOUSE. All right. Last, to follow up more on Senator Hatch's question, the issue of how the executive branch manages and administers its response to the cyber threat that we are facing is one that has been raised in dozens of pieces of legislation, and there are many different proposals. And I would urge you on behalf of the administration to take a position as soon as you can on how you would like to see it done, because every day there is a new proposal legislatively for how this should be done. Ultimately it is the executive branch that is going to have to implement, and the sooner the executive branch joins this debate in a meaningful way, the better off I think we will all be.

Mr. MUELLER. I will do that, although I would reiterate that if I look at our piece of it in terms of attribution for attacks, which we by necessity cannot do alone but must to with other agencies, I believe we have built a very strong platform that could be extended in the National Cyber Investigative Task Force.

Senator WHITEHOUSE. I agree.

I thank the Chairman.

Chairman LEAHY. Thank you.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman.

Director Mueller, I apologize for not being here for your testimony and for the other questions, but I did want to ask you a little bit about the High-value Detainee Interrogation Group, or HIG, and I understand that that has not been covered yet in questions.

Mr. MUELLER. It has not.

Senator KYL. Actually, the first question is: What is the status of it? And then I will have a second question as a follow-up to that.

Mr. MUELLER. Well, prior to its formal establishment in, I guess, the beginning of this year, the spring of this year, the concept had been utilized both overseas and within the United States, and by that I mean having a group of individuals available when an individual comes into the custody of either the military or some other counterparty agency or, indeed, with the United States custody in our custody, putting together teams that have both interrogation expertise, just in how you do it, but teams or participants that are familiar with the background of the individual, thoroughly familiar, thoroughly familiar with the subject matter, so that in the course of doing an interrogation you have not just from the FBI but from a number of contributing agencies the best in the way of expertise.

We have used that concept before the HIG was formally established. Right now I would have to get back to you as to how many people we have on board, but we have basically three components: one looks at the area of interrogation, the best practices and the like; one looks at training across the board; and the other one looks at how we operationally support interrogations around the world.

Senator KYL. Well, let me be a little more specific. My understanding is that it is under the direction—or the quotation here is "run by the FBI"—and headed by an FBI employee with two deputies, one from CIA and one from the Defense Department. Is that correct?

Mr. MUELLER. That is correct.

Senator KYL. It is also reported that there are three regional teams, locations not discussed, and I do not know that we need to

know how many teams there are or where they are. Could you just discuss that generally as to how quickly they could get to locations to perform their responsibilities quickly?

Mr. MUELLER. Well, if you anticipate the detention of somebody, it enables you to put the team together in anticipation of that detention. All too often what happens is somebody is detained, you did it by exceptional work by the intelligence community or otherwise, and so you very quickly have to put together the teams.

We have anticipated in various areas of the world that we may be called upon to put in a team, and so we have already lined up areas of expertise that would be available on a moment's notice should somebody be detained in that particular area of the world where we have got substantial concern.

Senator KYL. So the idea is to be able to respond very quickly with all of the expertise that is needed regardless of where in the world it might be.

Mr. MUELLER. Yes.

Senator KYL. And does that include the United States?

Mr. MUELLER. Yes.

Senator KYL. I recall there was some question about whether or not the HIG was intended to apply to interrogations in the United States. Admiral Blair expressed concern that it had not been properly set up to do that, but it has been now. Is that correct?

Mr. MUELLER. Within the United States, it would be ourselves generally that would conduct the interrogations, and we would make use of that capability and have made use of that capability already.

Senator KYL. Well, when you say "that capability," do you mean also Defense and CIA personnel with their access to their information sources that would be relevant to the interrogation?

Mr. MUELLER. Yes.

Senator KYL. So it is not just the FBI.

Mr. MUELLER. No. In each of the interrogations beginning, I think, back with the interviews with Headley in Chicago, you would have teams from across the intelligence community that would be participating in the interrogation, not necessarily asking the particular questions, although there have been occasions where it is not FBI agents who are asking the questions, but participating in that process.

Senator KYL. Right. What would you say is the primary—I am sure there are two or three goals here, but what is the primary goal of having the HIG?

Mr. MUELLER. I think it is twofold: the principal and essential goal is to gather as much intelligence as fast as possible that would prevent additional attacks; secondarily, to the extent possible to in the course of that intelligence obtain information that perhaps may be used as evidence in order to detain or lock up somebody else who may have been complicit. And, last, to the extent that there needs to be additional information that would assure the continued incarceration of that person, to make certain that you obtain that as well. But I do want to emphasize the principal priority is to gather intelligence to prevent future terrorist attacks.

Senator KYL. As to the third goal there, that could incorporate considerations, legal considerations relative to providing Miranda rights, for example?

Mr. MUELLER. Yes.

Senator KYL. Because of the need to have evidence that could, in fact, be used to detain the individual further or prosecute the individual.

Mr. MUELLER. Yes.

Senator KYL. But the first goal would not require that.

Mr. MUELLER. That is correct.

Senator KYL. And I have forgotten now what the second one was. I apologize. Repeat that again.

Mr. MUELLER. The second one was to gather information that will enable you to detain somebody else.

Senator KYL. Yes, further intelligence gathering, right. I got it. OK.

And just a final question here on this news of the release of thousands and thousands of e-mails, classified documents on a website. Is the FBI involved in an investigation there? And what do you anticipate the action of the Government would be relative to prosecution of both the individuals who provided the information and those who might have been involved in the dissemination of the information?

Mr. MUELLER. We are currently supporting the DOD investigation into that leak, and to the extent that DOD needs our assistance or we can be of help, we are providing that support at this juncture. I cannot say as to where that particular investigation will lead.

Senator KYL. OK. Just a final thing, back on the HIG again, if there is anything that you want to provide to us to more fully explain exactly how it is set up, that which we can easily discuss in public, to give us a more complete picture of exactly how it is set up, what it is intended to do, how it is going to operate and so on, who is involved, if you could provide that to the Committee, I think it would be very appreciated.

Mr. MUELLER. I would be happy to provide a briefing by the head of the HIG in which he can answer those questions you have and respond to any questions you might——

Senator KYL. Well, you responded very fully. I am not suggesting that you did not. I was just saying if you want to have——

Mr. MUELLER. No, he can do a better job in terms of fleshing out the details.

Senator KYL. All right. Great. Thank you, Director.

Chairman LEAHY. Thank you.

Obviously, on issues like this, anytime you would like to arrange especially the kind of briefings we have to do over in the SCIF, we are always happy to do that.

Senator Kaufman.

Senator KAUFMAN. Thank you, Mr. Chairman.

Thank you, Director Mueller, for being here, and thank you for your service, and I agree with everyone else. You are one standard, bright, consistent star that we know we can always turn to. I appreciate it.

Listen, Senator Sessions as usual raised some good questions about fraud and about the reduction in fraud from what we had earlier in the year, but I think a lot of what we discussed at the time just to confirm, when we passed the FERA, the Fraud Enforcement Recovery Act, that what happened here was that after September 11th, we moved a lot of FBI agents over to cover terrorism. In essence, we never backfilled those slots. Is that a pretty fair statement of what happened?

Mr. MUELLER. That is correct.

Senator KAUFMAN. And so that really when we went with the FERA Act, which had broad support, that is really -one of the objectives of the FERA Act was to try to go after fraud enforcement, get more FBI agents, get more prosecutors so that we could actually get back to the levels of fraud investigation and prosecution that we had early in the 21st century. Is that fair to say, too?

Mr. MUELLER. Well, yes, I would say that—again, I go back to what you noted. We have not been able to replace those that we moved over to counterterrorism in the wake of September 11th. But I will also say that we were doing a number of smaller cases that were distractions in terms of what we should have been focused on and pushing cases, white-collar criminal cases—anybody that has been a prosecutor knows that they take a long time to do, and you have to push them and push them and push them. And so the focus has been on prioritization as well.

Senator KAUFMAN. Right. And really it is a lot—the example I have used in the past is it is a lot like drug dealers. I mean, you can pick up a lot of drug dealers that have a small amount of drugs. Really what we are after is the drug kingpins. So what we would like to do is encourage you to go after the more complex cases, and especially in the fraud area where you have folks who—as has been stated in this Committee by witnesses, they cover their tracks a lot better than drug dealers cover their tracks, that while they are doing this, if you are involved in fraud, complex fraud of the kind we are talking about, they do a much better job of, as they go along, cleaning up after themselves so it makes it difficult for them to be prosecuted. We can find them, but then prosecuting them is a problem. And, second, they have access to some of the very best legal help in the country.

Mr. MUELLER. Yes, my admonition to my people, my suggestions to prosecutors is in some sense to treat white-collar criminal cases or handle them the same way you do drug cases; that is, identify the persons who conducted the wrong doing, gain the cooperation of one or more, and move up the line. Also, to utilize techniques that we have not necessarily used in the white-collar crime arena in the past, and that is Title 3s so that you can utilize many of those techniques that we traditionally have used against organized crime, against drug cartels and the like in the white-collar arena.

Senator KAUFMAN. We have had oversight hearings that included Lanny Breuer, who is the head of the Criminal Division, and folks from the FBI to talk about the idea of moving the more complex cases and using the very things that you have talked about. Correct?

Mr. MUELLER. Correct.

Senator KAUFMAN. Good. Can you tell us in securities fraud, which is one of the concerns that I have had in terms of—I think there is a lot of upset about what happened in the great securities meltdown, the loss of jobs, and the people losing their homes, the incredible difficulty people were faced with. And I think one of the examples, again, when we passed the Fraud Enforcement Recovery Act was to let people know that there is only one level of justice in this country, whether you are very, very wealthy and have a strong, complex legal team or whether you are someone else.

So where does securities fraud fit in terms of the priorities when you are trying to deal with fraud?

Mr. MUELLER. It is one of the top five priorities. White-collar is the No. 4 priority for us. And it is high there. We have almost 180 agents working solely on securities fraud as opposed to corporate fraud or mortgage fraud. And we currently have over 1,500 cases. We have had a number of, I think, successful prosecutions, the Petters prosecution out of Minnesota being one of them, the Galleon ongoing investigation in New York, and others where we have made a substantial impact.

If you look in terms of Ponzi schemes, quite obviously Madoff comes to mind, and there are others who are also spending substantial years in jail as a result of their fraudulent activities.

Senator KAUFMAN. And Galleon is a wonderful example of what you said earlier where someone came forward; you found someone who would testify and used them as a way to develop the case.

Mr. MUELLER. Yes.

Senator KAUFMAN. Last year, in November, President Obama set up the Financial Fraud Enforcement Task Force with the FBI as a member. How has the task force been doing?

Mr. MUELLER. The task force meets periodically, but its main thrust is to assure that we have at the same table periodically the individuals who are responsible in addressing fraud and to assure that we are working together.

For instance, one of the items that has been important to us is to assure that when records are subpoenaed by either the SEC or the prosecutor or come into the hands of the FBI, that we put those records in a data base that is searchable by each of our agencies as opposed to having to replicate different data bases when the case moves from agency to agency. And so not only a case that went through the SEC and through the FBI goes to the prosecutor, we are all working off the same data base of documents, which makes it much easier to investigate and a heck of a lot easier to prosecute.

Senator KAUFMAN. Great. And mortgage fraud, you have done a great job, and you had some really great successes in terms of dealing with brokers and the mortgage fraud. And I met with your folks in Los Angeles and other places, in Las Vegas, where there is that kind of—tell me a little bit how you move upstream from that. I mean, a lot of these mortgages were put together into mortgage-backed securities, residential mortgage-backed securities and the credit default swaps. That was one of the things that kind of drove the whole thing, as Senator Levin's Permanent Subcommittee on Investigations pointed out, was one of the key things.

How do you move upstream to go after the folks on Wall Street who were involved in the mortgage fraud?

Mr. MUELLER. Well, there are two levels. Certainly on the local level, where you have, say, an assessor, a buyer, a seller, a real estate broker, you focus on one of them to explain the scheme and provide the evidence that you need.

It is more difficult when mortgages are packaged and then sold as various investment vehicles to show knowledge on the part of those who are handling those investment vehicles as they pass hand to hand. But, again, it is a combination of obtaining the e-mail traffic, which often is very, very helpful, obtaining witnesses and in some circumstances utilizing a Title 3 wire to obtain evidence.

Senator KAUFMAN. I just want to tell you, thank you for your testimony and for your service. I just want to say those complex cases, I know they take a lot of time and effort, and I know that it is easier to maybe get the mortgage brokers' cases. But I just would encourage you to not go after the numbers but to go after the key cases, because I think that as I travel around the country and around Delaware, that is the thing that people are really upset about. Let us get some of these folks in these complex cases and put them behind bars. So thank you again.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you. Again, thank you for your work on the fraud legislation. You were, of course, a lead sponsor of that, and I think you shared my pride the day the President signed it.

We have talked about this before, the fact that—the selective cases, have some people who actually get hit hard, go to jail, you get a deterrent effect on it.

Senator Franken, you have been here patiently. Please go ahead, sir.

Senator FRANKEN. Thank you, Mr. Chairman.

Director, I share everyone's view. You have been—thank you for your service, and not just as Director of the FBI, which you have done stalwart, very effective work for now almost—well, 9 years, 9–1/2, but for all your service to this Nation.

I want to follow up on mortgage fraud and what Senator Kaufman was talking about and just get some kind of idea of what we are talking about here. You were talking about schemes with assessors and those kinds of things. In Minnesota, we are No. 2 in same-day house flips where someone buys and sells a home in 1 day, in the same day. And this often indicates some type of fraud is going on.

Is that a pretty common—what is going on there?

Mr. MUELLER. Well, actually about maybe a year ago, I had an opportunity to visit Minneapolis and talk about this particular area. I was looking at maps where there are swaths of territory that have gone way downhill as a result of mortgage fraud. Whether it be Minneapolis or elsewhere, data bases that show us that there are properties being flipped within 24 hours gives us an idea as to where to look. And so we utilize the data bases such as you have noted to put together a picture of persons who may be involved in a number of transactions in which there are one-day flips. And from there we will expand the investigation and determine

what is the common denominator in these one-day flips, and then we will follow up the investigation to determine who else was involved in what often—most times turns out to be some sort of scheme that is being perpetrated by a real estate broker, an assessor or somebody else in the——

Senator FRANKEN. So whether they are underassessing it and someone buys it and then overassesses it and sells it, or what——

Mr. MUELLER. There are a number of particular schemes that they can use. Generally the role of the assessor is to assess it higher than it is worth so that you get an increased mortgage, and so that the mortgage pays for the property; whereas, the seller or others believe that there is a downpayment being made, and so the whole property is being supported by the bank without the collateral that ultimately would make the bank whole.

Senator FRANKEN. What type of mortgage fraud is the most common? Are we still unraveling stuff from the predatory lending that was happening, you know, 4 and 5 and 6 and 7——

Mr. MUELLER. Yes. The answer is today we have over 3,000 cases, approximately 360 agents that are working on those cases. There are pockets in the country that have been hurt more than others, Las Vegas, Central Valley of California, just to mention two; but Phoenix and other cities have had—well, I would say had substantial issues with regard to mortgage fraud. In those cases, we put in place a task force. We will bring in the State and locals to participate on that task force. We have an inventory of mortgage fraud cases, and we will go down each of those cases and determine which ones we can pursue and which ones the State and locals can pursue, perhaps the State government, and try to work through that inventory to address each of them that has come to our attention.

Senator FRANKEN. Thank you. I also want to thank you for the Petters conviction. I know Senator Klobuchar and I want to thank you for that.

I want to get to a whole different subject. Over the last several years, we have heard a lot of speculation about what kinds of interrogation techniques work to draw out the best and most reliable information. And I want to ask you, from your experience as FBI Director—you started just the week before 9/11—what kinds of interrogation techniques do you think work best when dealing with terrorist suspects? Which kinds of techniques yield the most helpful and reliable information?

Mr. MUELLER. I did not have the opportunity to spend time as an agent myself doing interrogations. I was a prosecutor, and you could say that some of the questioning that you do falls in that category. But I rely on the experts within the Bureau, and the longstanding Bureau practice, we focus on rapport building—rapport building with the obtaining of collaboration—corroboration, I should say, corroboration with regard to whatever statement is being given. And that has been our practice for any number of years, and that is the practice we have followed over the last 10 years and presumably will be the practice we follow in the future.

Senator FRANKEN. Because I think some Americans, you know, question the use of so-called enhanced interrogation techniques, and I think they are—hopefully they are history. Do we get more

reliable information from the kind of questioning the FBI has done or from the enhanced—from your judgment?

Mr. MUELLER. I am not certain that I am a person who can be definitive. All I can say is that we find our techniques very effective, and we do believe we get reliable information, but it is a combination of information that you obtain, knowing a great deal about the individual, having corroborating evidence to know that what you are getting is the truth, and it is a process—not just a process of questioning, but a process of developing rapport, developing information, and taking it step by step to assure that you are getting all that that person has, or to the extent that you can, and that it is accurate information.

Senator FRANKEN. My time is up, and I will submit in writing a question about trafficking from Indian reservations. The last time I did ask you about that, and I want to thank you for following up with me on it. I appreciate your work in that regard.

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

Senator FRANKEN. Thank you, Mr. Chairman.

Senator WHITEHOUSE. We turn now to Senator Specter.

Senator SPECTER. Thank you, Mr. Chairman.

Director Mueller, I join my colleagues and again welcome you here.

Mr. MUELLER. Thank you, Senator.

Senator SPECTER. As part of the Judiciary Committee's oversight of the FBI, I have inquired about the investigation of former Congressman Curt Weldon where there was a search-and-seizure operation at the home of his daughter a few weeks before his reelection effort in 2006. And the television cameras arrived before the FBI arrived with the search-and-seizure warrant, and the consequence was that Congressman Weldon was defeated. And the FBI conducted an investigation as to the leak, and four representatives of the Department of Justice had contacts with the news media. None was polygraphed, and there was not an effort made to pursue the source of the leak as intensity as you do in national security cases.

My first question is: Is it the customary practice of the FBI to give polygraph examinations to people who have had known contacts with the news media in a situation like this?

Mr. MUELLER. I am not familiar with the case in which there is a relatively large universe of persons who may have disclosed the information where we would do polygraphs across the board. I am familiar with situations in which we may have a suspect——

Senator SPECTER. I am not asking about polygraphs across the board. I am asking about four DOJ people who had known contacts with the media.

Mr. MUELLER. I do not have—I am not familiar with the circumstance where we would have done polygraphs—required polygraphs of four individuals.

Senator SPECTER. So you say it is not the FBI policy to polygraph.

Mr. MUELLER. It is not. It is used on a case-by-case basis.

Senator SPECTER. The briefing that I had, the briefers told me that on a matter of this sort, the issue is not pursued with the same intensity as in national security. For example, there were no

questions asked of the newspaper reporters who published stories in McClatchy and in the Washington Post. Why not?

Mr. MUELLER. I am not certain that is the case. I know you were briefed by attorneys from the Department of Justice, and I am not certain what the rationale would be for not asking them questions. I would be, I think, surprised if they answered those questions, but certainly the questions generally are and should be asked.

Senator SPECTER. Well, I wrote to you about this matter on July 22nd, so there has not been a whole lot of time. I infer you have not seen the letter.

Mr. MUELLER. No, I have seen the letter, sir, and I have looked at the letter, and many of the questions are—I think there were three questions you asked there, and I do believe the questions really are those to be answered by the Department of Justice who was handling the prosecution. Your question, for instance, about why we did not press and subpoena the reporters really goes to a determination in the Department of Justice where there is a balancing that takes place as to whether or not you do that.

Senator SPECTER. Well, the investigation on the FBI leak was conducted by the FBI, wasn't it?

Mr. MUELLER. I believe we did undertake an internal investigation, yes. But the overarching investigation, the criminal investigation, was conducted by the U.S. Attorney.

Senator SPECTER. Is it a crime to leak?

Mr. MUELLER. It certainly can be, yes.

Senator SPECTER. Well, was it in this case?

Mr. MUELLER. I would have to go back and look at the facts and circumstances.

Senator SPECTER. Well, it is a game of ping-pong. It took a long time to play this game, about 4 years so far. But when you have a Member of Congress involved, you have a very sensitive matter. The briefers told me that this matter was not investigated by pursuing the sources with the intensity that sources are sometimes pursued. It depends upon the importance of the investigation. If it is a key national security interest, then the sources are pursued, even to the extent of a contempt citation.

You and I have differences of opinion as to the shield law which I have proposed and which has not yet been acted on. But as long as you have procedures for pursuing sources, I believe this is the kind of a case where sources ought to be pursued, that it is a very, very serious matter, like a national security matter. And I say that because of the separation of powers. Congress has the oversight responsibility to investigate the FBI, and the FBI appropriately has the responsibility to investigate Members of Congress if there are allegations of bribery, for example.

But it seems to me that where you have separation of powers and you have the chilling effect that an FBI investigation has on a Member of Congress like Curt Weldon, it ought to be handled with the greatest intensity possible to pursue the sources if you can.

Would you disagree with that?

Mr. MUELLER. Senator, I think we are on the same page, and I would venture to say in a case such as this, the agents who were handling would very much want to have pursued the sources. One

of the ways to pursue the sources is to ask the persons who published the pieces or the persons who triggered that.

As you are well aware, there is a process that you go through in the Department of Justice to gain approval to even contact a person in the media who may have developed source information and taken some action on it.

Senator SPECTER. Well, my time is up, but that was not done, and the briefers told me they did not even question the cameras that arrived. That was news to them. Would you take another look at those issues, Mr. Director?

Mr. MUELLER. Yes, sir.

Senator SPECTER. One more comment, Mr. Chairman. I will not be too much longer. I asked the briefers if the investigation was over, and I was not surprised that they did not tell me. I am not going to ask you a question. I am just going to state the proposition.

It seems to me that when years have passed, people under investigation ought to be told if the investigation is over, and I know you have a policy of not doing that. And it seems to me—and I used to be in this line of work, so I understand the investigation—you do not tell people it is over because it may not be over. Well, it may not be over if new information is acquired, but if there are no undeveloped leads outstanding, it seems to me that the FBI ought to tell people that it is over so the Sword of Damocles is gone. And if something new comes up, they can always start it again.

Do you disagree with that approach?

Mr. MUELLER. No. What I would say is that it is not necessarily us, it is the prosecutors that make the determination when the investigation is closed, and there is a procedure in the Department of Justice for a defense attorney to ask whether or not their client remains a subject or target of an investigation. And in most cases, the Department will respond, either affirmatively or negatively to that letter. But there is a process that is in place to accomplish what you are alluding to.

Senator SPECTER. Thank you.

Senator WHITEHOUSE. We will now recognize Senator Klobuchar, followed by Senator Durbin, and I believe Senator Kohl would like to have a brief second round, and with time permitting, we will then go to Senator Kohl unless other people intervene for their first round.

Senator Klobuchar.

Did I say "Kohl?" Kyl. Senator Jon Kyl of Arizona. My apologies.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman, and thank you, Director Mueller. It is good to see you again.

I wanted to start out by commending your agents for the great work they did on that Tom Petters case. I think people were very focused, understandably, on the Madoff case, but this was the second biggest one in the country, an unbelievable loss of money in our State with so many people, including nonprofits that had invested, and it was very complicated. And it was an enormous victory, and everyone was prosecuted. So I want to thank you for that.

Mr. MUELLER. Thank you, ma'am.

Senator KLOBUCHAR. I know the top priority, as many people have talked about, is the work that needs to be done and continues

to be done with terrorist threats in this country. But I wanted to focus on something I know Senator Whitehouse talked about a little, and that is, cyber crime and cybersecurity, which is not only necessary for our national security, but also to the economic and physical security of ordinary Americans.

We all know that the Internet is a powerful tool, but in the wrong hands, it can also be a powerful tool the other way, for not good reasons. And my concern is that the predators have become more sophisticated than the laws that we have on the books, and I am going to use—one example is a bill that I am introducing in the next few days, a bipartisan bill on the stalker bill, and this is called the Stalking Act of 2010. It has already passed the House. We did an event yesterday with Erin Andrews, the ESPN reporter who was videotaped by a Peeping Tom who reversed the peephole in the door and then got that video out on the Internet of her changing clothes, and it went everywhere. And she is maybe a celebrity, but there are so many other people, including people in my own State, that have been victimized by this one guy, ended a relationship on the Internet, and he ended it and he was mad at the woman so he put all of her personal identification information and her children on porn websites asking people to rape their kids. He was convicted and sentenced.

So what I would like to know—I hope that the FBI will be supportive of this bill that we have or be helpful in getting it done. But I want to know, Do you think that there is a need to modernize our criminal laws to keep pace with the new technologies? That is something we do in this bill. And are there particular areas that you think Congress should be focusing on when we look at some of the modernization of our statutes that needs to take place to keep up with these predators and also white-collar criminals that are using the Internet?

Mr. MUELLER. Let me start by saying I understand that the bill that you are suggesting will identify particular conduct and then have strong penalties for engaging in that conduct. Not being familiar with the bill myself and deferring to Justice for the opinions letter, nonetheless this is something that is badly needed. I venture to say in 10 years much of the discussion at a hearing like today, maybe 80 percent of it will revolve around the Internet and cyber as opposed to maybe 20 percent of it now. And our laws are antiquated in the sense that they were developed to address conduct or equipment such as telephones and telephone lines and the like, and there is a great need to update them to continue to give us the authorities that we need to do our work, but utilizing the new modalities in order to accomplish that.

Senator KLOBUCHAR. We look forward to working with you on that, you know, even beyond the stalker issues. And in your testimony, you actually discuss the cyber attack on Google late last year, and this attack I believe highlights the growing security risk that we have in this country, which is cyber attacks that could actually potentially cripple our infrastructure. We are not here talking about, you know, one stalker out there in a hotel room. Here we are talking about actual threats to our national security and our infrastructure.

What is the FBI going to do to address these kinds of threats? And what should we be doing here in Congress?

Mr. MUELLER. The task force that I alluded to before, the computer task force that we have with 14 or 15 other agencies is a very good first step in my mind. And as I said before, particularly when it becomes necessary to protect our infrastructure, there are lessons within the Federal Government that can be learned from persons in the Cyber Command, for instance, that are applicable to protecting the Government across the board, whether it be Congress or the Supreme Court or the various Government agencies.

The more difficult problem becomes the dot-com and the networks that are not subject to legislation necessarily, but need as well to be protected because so much of our financial information goes out over these particular Internet wires. And to the extent that we can identify, isolate, and protect the backbone cyber structures of the United States, we need to do that. But then the next level is protecting businesses who utilize dot-com and the like as opposed to dot-gov, dot-mil, and the Government areas.

We play a role in protecting the Government and determining the attribution of particular attacks. We would want to see that role expanded. But we do not necessarily play the role. DHS plays a role in protecting the Internet apart from the dot-gov, dot-mil, and the rest of the governmental structure.

Senator KLOBUCHAR. Now public-private partnership is vital to the development of a comprehensive, innovative solution that improves and expands our Nation's capabilities and keep us ahead of these emerging threats. I am convinced of that from my work as a prosecutor that a lot of this was being able to work with private entities who are controlling some of this data.

What is the Department doing to work with the private sector? And what more can we do to create incentives for private businesses and institutions to work with Government on cybersecurity issues?

Mr. MUELLER. We have got a number of initiatives to do just that. Out in Pittsburgh, working with Carnegie Mellon and others, we established partnerships that enable us to exchange information on the latest worms, viruses, attacks, and the like. We have a wide-ranging group of individuals whom we consult with and who alert us to new things that are happening.

But I will say in the same breath that you to a certain extent have to be careful. You cannot have the private entities acting as an agent of the United States. On the one hand, you need the expertise and the cooperation, the collegiality; but on the other hand, when it comes to doing and conducting investigations, it needs to be the Government and not fall into a role where private industry is working so closely with Government that it becomes an agent of the Government. And so it is just a cautionary tale.

Senator KLOBUCHAR. How about a BP issue? You do not have to answer that.

So I understand that, but I also think the expertise—somehow we have to get that expertise and use it, because I just think that we are at the tip of the iceberg with some of these things we are seeing recently that have happened, and we look forward to working with the Department on improving our laws, both with the

stalker one I mentioned, but in a much bigger way with security issues. So thank you very much.

Mr. MUELLER. Thank you.

Senator WHITEHOUSE. Senator Durbin.

Senator DURBIN. Director Mueller, good to see you again.

Mr. MUELLER. Sir.

Senator DURBIN. About 6 weeks ago, I attended a funeral in Chicago. It was a young Chicago police officer named Thomas Wortham, 30 years old. He had served in Iraq. An extraordinary young African American with a great life ahead of him. Gunned down in front of his home, in front of his father's home. His father, a retired policeman. They were armed as security would require and as their jobs required, and still he was shot down and killed.

Last week, Michael Bailey, another Chicago policeman, left his detail guarding Mayor Daley and went home and at 6:30 in the morning was polishing off his new Buick that he could not wait to drive around when he retired in just a few weeks, and a man came up and shot and killed him.

We have lost three policemen in Chicago in the last 2 months. The gun crime there is sadly aggravated by the hot weather. Just terrible the loss of life that we are experiencing.

There has been an exchange between the mayor of Chicago and Robert Grant, your Special Agent in Charge, whom I know and respect very much. And I think at the end of the day it reflected the frustration they both feel. Everybody is trying everything they can think of. And my request to you is: Can you help us in finding some new ways to go after the illegal guns in Chicago, the violence on our street? Is there something the FBI can do to help us in the city?

Mr. MUELLER. I am familiar with all three of those instances. I called Jody Weis, who is the chief of police, after the third one, not only with my condolences but also with is there anything more that we can do. Rob Grant is one of our best, most effective, and most longstanding Special Agents in Charge who feels deeply about the necessity for reducing the violence in Chicago.

We have tried across the country a variety of techniques. My belief is that in Chicago we have tried just about every one of them. Rob Grant is on the cutting edge of utilizing whatever intelligence we can gather to try to focus on the shooters and put them behind bars. I will again go back and have a discussion with him. I believe he is in town, but have yet another discussion with him.

We have added resources, I know, in the office there to address this, but in comparison to the extent of the problem, it is inadequate. And so we will do what we can.

Senator DURBIN. If you will tell me what you need, I will do everything in my power in the Appropriations Committee to help. It is just heart-breaking. And as Thomas Wortham's father said to everyone in Chicago, "If they will shoot us down in uniform as policemen, armed, they will kill anybody." And that is the feeling many of us have, that we have to really do much more to try to bring this under control.

I in the past have been complimentary of you and the efforts of the FBI since 9/11 to deal with the Arab and Muslim population in America. I thanked you, commended you for making it clear that

we are not casting a wide net and saying that those of Arab descent or those of the Muslim faith are necessarily to be suspect; and also to suggest, as you have before this Committee, that the cooperation of Arab Americans and Muslim Americans is critical to bringing in the information. We need the intelligence. We need to stop future acts of terrorism.

There has been a recent article in the New York Times which questioned the current situation at the FBI. It was entitled, "Muslims say FBI tactics sow anger and fear."

The terrorism expert David Schanzer said, "This is a national security issue. It is absolutely vital that the FBI and the Muslim American communities clear the air and figure out how to work together." And Michael Rolince, a former FBI counterterrorism official, said, "There are some people in the Bureau who believe as I do: The relationship with the Muslim community is crucial and must be developed with consistency. And there are those who don't."

One of the things that is still being debated, or at least considered for change, were some guidelines handed down by former Attorney General Mukasey concerning the assessments of innocent Americans, whether there is a suspicion of wrongdoing, and this is a source of concern in the urban Muslin community.

Now, I know the new Attorney General, Eric Holder, pledged that he would review these Mukasey guidelines. Are you familiar with this Domestic Investigations and Operations Guide, DIOG?

Mr. MUELLER. Yes, absolutely.

Senator DURBIN. And it is my understanding it is unclassified?

Mr. MUELLER. It is unclassified; however, we have withheld certain portions of it from publication because it would give individuals an insight into how we operate. But I will say as we develop these guidelines—we fully briefed Congress. Congress has seen the guidelines.

Senator DURBIN. What Members of Congress?

Mr. MUELLER. Judiciary Committee when the guidelines were being developed, we had extensive meetings with staff of the Judiciary Committee. We had suggestions as to how to change the guidelines from the Judiciary Committee, both Judiciary Committees in developing these guidelines.

Senator DURBIN. Did you provide a copy to the Senate Judiciary Committee?

Mr. MUELLER. I believe we did.

You have seen a copy. You have seen copies.

Senator DURBIN. OK. We do not have a copy. I imagine that is the difference here. The question is whether we get a chance to review it.

Let me ask you this: Is there a requirement of suspicion of wrongdoing before there is surveillance of an individual or surveillance of a location?

Mr. MUELLER. Yes.

Senator DURBIN. All right. And so merely the fact that it is of a certain religious sect or ethnic group is not enough.

Mr. MUELLER. That in and of itself is not enough. There has to be something more.

Let me just allude to one thing you said about the relationship with the Muslim community. I think it has maintained its positive note throughout. There are segments in the Muslim community that do not necessarily want the relationship to work out. But in every one of our 56 field offices, we have since September 12, 2001, had outreach to the Muslim community. And if you walk around and you talk to individuals in the Muslim community, the leaders in the Muslim community, you talk to our Special Agents in Charge, I think almost one of you will find that the relationships are very good.

Now, there are distinct pockets where they do not want to see that relationship succeed, but I believe that that relationship has grown and improved and that the Muslim community understands that it is not just the FBI that is responsible for keeping this country safe, but all Americans, including the Americans who happen to be Muslim.

The last point I would make is that the guidelines—we work with the new administration day in and day out in our investigations that are administered according to these guidelines. I believe they are effective. I think they are appropriate, and I think they are the appropriate balance between civil liberties on the one hand and giving us the tools we need to protect the American public against terrorist attacks.

Senator DURBIN. My time is up, but if I could just say in closing, for 8 or 9 years you and I have had an ongoing dialog about the new computer technology at the FBI. There have been some ups and some notable downs, and I know there is a new Inspector General's report about your Sentinel system, and I will send you some written questions and follow up——

Mr. MUELLER. And I would be happy to sit down and brief you on where we are and where we are going.

Senator DURBIN. Thank you very much.

Mr. MUELLER. Yes, sir.

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

Senator WHITEHOUSE. Thank you.

Senator Kyl, I know this is the second round and you will be going ahead of Senator Schumer, but he has said that if you will be brief, he is more than happy to accommodate you.

Senator KYL. Thank you very much. I just had two questions. One is a follow-up on—and thank you, Senator Schumer. One is a follow-up on the HIG.

I had reference to a letter dated February 3rd of this year to Senator McConnell relating to the Northwest Airlines Christmas bombing event and related policies of the Department of Justice and the FBI. And with regard to interrogation, there is one paragraph in here that I thought might conflict with what you said about the three goals with respect to the HIG, whether abroad or in the United States, and I just wanted you to be able to clarify that.

In this letter, you say, and I quote, "The FBI's current Miranda policy, adopted during the prior administration, provides explicitly that within the United States Miranda warnings are required to be given prior to custodial interviews."

Now, there is a footnote right there which describes the Quarles exception in cases—and it is quoting, "The warning and waiver of rights is not required when questions which are reasonably prompted by a concern for public safety are asked," and then you give an example.

But the reality is that the HIG interrogation about potential future terrorism plots or plans do not really and easily fall within the Quarles exception in many cases because it is not a matter of—an immediate matter of public safety. Is that not correct? And so could you describe what the policy is with respect to the Miranda warning in domestic HIG interrogations?

Mr. MUELLER. Well, I think the fact that it is in a footnote—it probably should be elevated because we have adjusted it to address terrorist cases. Originally the Quarles exception, as I think you know, is related to a robbery and was much more discreet. There has been no elaboration on the extent of the Quarles exception, and, consequently, in bringing that over and adjusting to the terrorism arena, there is a breadth of interrogation that inevitably would take place that goes well beyond what happened on that particular day on that particular plane, which legitimately in my mind falls within the Quarles exception.

I can tell you that in the wake of the Christmas Day bombing, for instance, we have educated our workforce, including the SACs, in terms of the Quarles exception so that it is on everybody's mind that when somebody is detained here in the United States, you have an opportunity to spend what time is necessary to gather the information on potential threats.

What triggered this was what happened on December 25th with 253 coming in from Amsterdam. In that particular case, as I know you are aware, the agents determined that they needed to interrogate Abdulmutallab immediately without Miranda warnings to obtain exactly that kind of information. There may be some disagreement as to how far you go, but in the terrorism context, I am comfortable that we will be asking the questions that are necessary to the public safety.

Senator KYL. That is very helpful, and I think it would be worthwhile to describe a little more fulsomely, to the extent that it is possible to do so, in these sort of hypothetical situations. But it is clear that you would need a broader interpretation of the Quarles exception in these terrorism cases, and, in effect, what you are saying is that you do interpret that exception in a broader context in trying to interrogate people about these terrorist threats. Is that correct?

Mr. MUELLER. That is correct.

Senator KYL. Yes, thank you.

The other question I wanted to ask you has to do with the Lockerbie bomber, al-Megrahi. I was very impressed with the letter that you wrote to Scottish Justice Minister MacAskill when you learned of his released, and I just wanted to quote a little bit of it because I think it is quite appropriate. You said that his action in releasing Megrahi is "as inexplicable as is detrimental to the cause of justice. Indeed, your actions make a mockery of the rule of law. Your action gives comfort to terrorism around the world who now believe that, regardless of the quality of the investigation,

the conviction by a jury after the defendant is given all due process and sentence appropriate to the crime, the terrorist will be freed by one man's exercise of compassion."

And you also went on to fault Scottish authorities for "never once having sought our"—meaning the FBI's—"opinion, preferring to keep your own counsel and hiding behind opaque references to the need for compassion."

Also at the time, President Obama announced that he was surprised and disappointed and angry to learn of his release.

But just last week, or maybe earlier this week, we learned that the State Department actually was consulted in advance, and, in fact, one Richard LeBaron, deputy head of the U.S. embassy in London, wrote to Scottish authorities on August 12th, just before Megrahi's release, saying, and I quote, "We greatly appreciate the Scottish Government's continued willingness to solicit the views of the United States and the families of its victims with respect to a decision on Megrahi's transfer," and then later, even offered qualified support for "conditional release on compassionate grounds."

When did you first learn of that State Department letter; do you know?

Mr. MUELLER. When it was in the newspapers.

Senator KYL. And was the FBI given an opportunity to weigh in or object prior to the letter being sent?

Mr. MUELLER. I had conversations with the Attorney General beforehand. I do not think there was any question but of the position that the Bureau felt strongly about and the Department of Justice felt strongly about. I think it was a shock to everybody that the decision went the way it did.

Senator KYL. I was very surprised, too, and that is why I do not quite understand how you could have the President being surprised and—what did he say?—surprised, disappointed, and angry, and have you say what you said, which I thought was very appropriate, and yet the State Department knew before then and acknowledged that it was being consulted.

Can you explain or has there been an explanation subsequent to this that maybe you could make us aware of?

Mr. MUELLER. No, and when, I think, I alluded to in the letter that we had not been consulted, I meant the investigators who had spent so much time. I was speaking for the FBI. We had spent a great deal of time with the families, investigating that case, with our colleagues overseas, and generally in such cases when you spend so much time on an investigation, those who conducted the investigation are queried as to what the disposition should be. That did not happen in this case.

Senator KYL. Right. And it is clear in what you said; that is exactly what you meant. Thank you very much, Director.

Senator WHITEHOUSE. Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. And thank you for your service, Director Mueller.

I am concerned a little bit about prepaid cell phones. It is too easy for both would-be and successful criminals to use cell phones, prepaid cell phones anonymously to accomplish their ends and evade detection. Recently Faisal Shahzad, the Times Square bomber, made use of a prepaid cell phone, among other things, to call

Pakistan, arrange the purchase of the Nissan Pathfinder that he rigged to kill as many people as he could on a busy Saturday night in Times Square. It was only because of a lucky break that authorities were able to trace him.

The devices were also used to transmit information in the Galleon insider trading scheme, a different type of crime. Criminals of all types know they are anonymous and virtually untraceable. They can hide away from law enforcement's appropriate reach.

So here is my question: Does the anonymity of prepaid cell phones pose law enforcement problems in a variety of cases as these and other anecdotes suggest?

Mr. MUELLER. Yes.

Senator SCHUMER. Could you elaborate just a little bit?

Mr. MUELLER. As you said, criminals, terrorists, persons who for whatever reason want to avoid detection, can use throwaway cell phones at will, which minimizes the capability we have to intercept those conversations that are often essential to a successful thwarting of an attack or——

Senator SCHUMER. I suppose as times goes on, more and more criminals are going to learn that this is sort of the way to go to avoid detection, particularly if they are in areas where there might be detection: terrorism, organized crime, financial crimes, things like that.

Mr. MUELLER. Yes, sir.

Senator SCHUMER. OK. So I have sponsored a bill—this is a nice bipartisan note with Senator Cornyn, my colleague on the Judiciary Committee—that would require purchasers of prepaid cell phones to present ID, just the same way that purchasers of monthly cell phone service have to do. The information would be kept by the wireless carrier who would retain it, with the same privacy protections that we have when we register for cell phones for 18 months.

Now, I know that you have to go to the great Justice Department to get the official OK on a piece of legislation, but would you agree that requiring prepaid cell phones would enable you to quickly and accurately investigate myriads of cases that involve prepaid cell phones as instrumentalities of crime?

Mr. MUELLER. Yes.

Senator SCHUMER. What is the most you can say about such legislation that Senator Cornyn—without getting yourself fired or anything like that?

Mr. MUELLER. I think I can say that, without having seen the specifics of the statute, we would be very much supportive of that kind of reporting requirement, and it would be indispensable, goes too far, but essential to the success of a number of investigations and cases that we would have.

Senator SCHUMER. Thank you.

I would like to go, since I have a little more time here, to narcotics on the northern border. New York, of course, has a long border—peaceful, generally—with Canada. A few days ago, the FBI announced very positive results as part of Project Deliverance. This was involved with the Mexican border, drug-trafficking organizations in the U.S., and involved coordination—FBI, ICE, DEA. You

arrested thousands of individuals, seized about $154 million in currency.

However, what is overlooked is that our northern border also faces a drug-trafficking epidemic, especially involving trafficking of different kinds of—some are the same, some are different—Ecstasy, marijuana, crystal meth. They have invaded our communities, particularly in upstate New York.

So I have introduced legislation to try and get the Federal law enforcement agencies to develop a comprehensive northern border counternarcotics strategy. I am not asking you explicitly to support this legislation. I will quit while I am ahead. But do you think that we could benefit from such a strategy? And will the FBI work to try and bring a Project Deliverance effort to the northern border generally and New York specifically? How can we work together to make this a reality? It is becoming a more and more serious problem.

Mr. MUELLER. Certainly the cooperation of Federal, State, and local entities along the border is essential to the safety of the border. To the extent that we can and should play a role, we definitely would play a role. I would be surprised if there is not already a strategy that one could buildupon.

Senator SCHUMER. Exactly. There is some cooperation, and we have gotten a little more attention in the past, but we could use a lot more, as you said, and I would hope that you internally would importune the powers that be to do so, as I am doing externally. But I am glad you say it would be helpful in terms of stopping drugs and stuff like that.

Final question, Internet fraud. You mentioned in your statement it is a growing concern for legitimate businesses. According to the Internet Crime Complaint Center, a partnership between the FBI, the White-Collar Crime Center, and the BJA, Bureau of Justice Assistance, a great many of these schemes, such as auction fraud, Nigerian 419 schemes, fraudulent high-yield investment programs are facilitated by, again, anonymous wire transfers that are hard to trace, almost impossible to reverse, and generally provide little or no fraud protection.

Have wire transfers made the FBI's job more difficult in going after fraudsters? What tools would help the FBI enforce the existing fraud laws in anonymous wire transfers while protecting consumer needs? And I will just give you one example and then you can answer the question.

Earlier this month, the New York Times reported on Internet scammers setting up fake Web sites pretending to sell used cars. They got the money; there was no car. They used Moneygram. Moneygram said the money had been collected on June 12th, but then told law enforcement, "We are not responsible for third-party fraud," and they would not even tell law enforcement—I am not sure if it was the FBI in this case, but in all likelihood, it probably was. They could not even tell them where the money was picked up unless you supplied a subpoena.

What are you doing about these types of cases? What can Congress do to help the FBI and consumers protect themselves?

Mr. MUELLER. Well, to the extent that we are notified either through the IC3 or otherwise, we will handle investigations or

work with State and local law enforcement to address a particular investigation. But it does not go to—that does not really answer your elemental question about what about anonymous wireless financial transfers. That is a growing concern throughout the world, not just the United States.

The immediate response would be requiring passing legislation that would require the presentment of identification and keeping records that would be available pursuant to a subpoena down the road, in the same way that you suggest, doing that for throwaway cell phones.

Senator SCHUMER. Right.

Mr. MUELLER. The ability to obtain records of past transactions is absolutely essential, whatever the method of payment or communication.

Senator SCHUMER. Well, it is legislation I am looking into, so I am glad you are positively disposed to at least exploring it. And, again, the one thing I would say before turning things over—my time is up. We are not expanding—or impinging on anyone's privacy rights. These are the exact same privacy rights people have when they do give their names, and there are lots of safeguards that, in my judgment, have worked quite well over the years.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Thank you, Director. This brings the hearing to a close. The record of the hearing will remain open for a week for any additional materials that anybody wishes to submit. As always, your testimony is helpful and candid, and we appreciate you being here.

Mr. MUELLER. Thank you.

Senator WHITEHOUSE. The hearing is adjourned.

[Whereupon, at 12:16 p.m., the Committee was adjourned.]

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

QUESTIONS AND ANSWERS

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 21, 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 July 28, 2010. Please note that these responses are current as of October 4, 2010.

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 July 28, 2010, Hearing Before the Senate Committee on the Judiciary Regarding Oversight of the FBI

Questions Posed by Senator Feinstein

Drugs and Mexico Border Violence

Mexican President Felipe Calderon last year signed a law legalizing possession of small amounts of marijuana, heroin, opium, cocaine, methamphetamine and LSD for personal use, three years after the country abandoned a similar plan under pressure from the Bush administration. Mexico says the new law frees it up to go after major criminal cartels that move billions of dollars of narcotics into the United States, the world's top illicit drug market.

1. Do you believe that the changes in the law enacted in Mexico are going to have an impact on the escalating violence along the southwest border and what is the FBI prepared to do in order to counter any escalating violence?

Response:

It is too early to know how Mexico's new drug law, which decriminalizes drug possession in certain circumstances but mandates treatment for repeated possession, will affect drug-related violence in Mexico. Notwithstanding this new law, though, it appears that the major Mexican criminal enterprise organizations may be attempting to increase revenues by expanding their involvement in such criminal activities as kidnapping, extortion, weapons trafficking, auto theft, and illegal alien smuggling. To combat the violence along the Southwest Border (SWB) and the possible spillover onto U.S. soil, the FBI is reviewing the possibility of placing additional Special Agent and Intelligence Analyst resources in SWB field offices. The FBI believes that by creating hybrid squads (which are discussed in more detail in response to Question 4, below) in key border offices, we will be better able to develop investigations and intelligence across field offices and programs and to dismantle the most egregious criminal enterprises.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00049 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.002

2. In the 2009 National Southwest Border Counternarcotics Strategy an emphasis is placed on providing information to local law enforcement along the border. What efforts are being made by the FBI to achieve this goal?

Response:

The Southwest Intelligence Group (SWIG), created by the FBI in 2009, serves as a clearinghouse for intelligence and situational awareness along the SWB. The SWIG, which is currently housed at the El Paso Intelligence Center (EPIC), produces both strategic and operational intelligence in support of the eight FBI SWB field offices and shares pertinent Mexican Drug Trafficking Organization information with state and local entities along the SWB. One full-time Senior Executive Service FBI Agent and eight Intelligence Analysts have been assigned to the SWIG to ensure that daily intelligence products are effectively disseminated throughout the FBI and the other participating EPIC agencies.

The FBI's counter-drug efforts are also coordinated closely with the EPIC to ensure proper de-confliction and to facilitate information sharing. The FBI co-chaired the Anti-Drug Intelligence Community Team (ADICT) working group regarding Mexican spillover violence, which produced two intelligence products on this issue. The unclassified version of this report is disseminated to our state and local law enforcement partners.

In addition, an Organized Crime and Drug Enforcement Task Force (OCDETF) Co-located Strike Force was created in El Paso and is now comprised of 12 FBI Agents, 16 Drug Enforcement Administration Agents, 6 Immigration and Customs Enforcement Agents, and a total of 9 other investigative agents from a variety of Federal and state law enforcement agencies. The FBI also continues to participate in other OCDETF Co-located Strike Forces along the SWB that include substantial numbers of state and local law enforcement participants, in San Diego, Phoenix, Tucson, and Houston. The FBI provides case updates and other information to the OCDETF Fusion Center to ensure that accurate and timely information from FBI cases can be fused with pertinent information from other organizations, including other Federal law enforcement agencies, to produce operational intelligence products that link investigations and facilitate the targeting of priority criminal organizations. This information is also included in quarterly reports on Mexican Consolidated Priority Organization Targets and Regional Priority Organization Targets that can be disseminated to state and local entities. The FBI also disseminates Situational Intelligence Reports and

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.003

Intelligence Bulletins through Law Enforcement Online in order to share area-based strategic intelligence trends with state and local entities.

In addition to these efforts, the FBI has continued its active participation in the High Intensity Drug Trafficking Areas (HIDTA) program, which is designed to enhance and coordinate drug control efforts among local, state, and federal law enforcement agencies. We are also the lead agency in the San Diego/Imperial Counties Terrorism Related Drug Initiative and we work in Arizona with the Tohono O'odham Nation, which sits on the Mexican border. Additionally, we participate in various intelligence centers that are critical to effective information sharing regarding drug offenses and other criminal activities. These include the McAllen Intelligence Center, which operates under the South Texas HIDTA to provide tactical and analytical support to surrounding federal, state, local, and tribal law enforcement entities.

3. To what extent has the FBI been able to work with the Government of Mexico to investigate kidnapping for ransom cases with a cross-border connection? Have you seen a rise in the number of cross-border kidnappings this year?

Response:

The FBI has worked well with the Government of Mexico to investigate kidnapping-for-ransom cases, appointing Border Liaison Officers who work closely with their Mexican law enforcement counterparts to achieve the release of kidnap victims from their captors. The FBI has trained Kidnapping Investigative Units for five Mexican states (Chihuahua, Baja California, Nuevo Leon, Coahuila, and Zacatecas) and plans to train units in five more states. The trained units have already begun to exert a positive impact, having already assisted the FBI in investigating kidnappings of U.S. citizens.

The FBI has not seen an increase in cross-border kidnappings in 2010. As of 9/1/10, the number of cases opened in our SWB field offices was on pace to be below the number of cases opened in 2009. This year's decrease follows four straight years of increases in the number of SWB kidnapping cases.

FBI Hybrid Squads

FBI Hybrid Squads co-locate FBI personnel with different types of expertise to address threats such as cross border drug violence. These squads, which are currently deployed in San Diego and Phoenix, have proven effective, especially when they coordinate with state

---

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.004

and local partners. I believe such collaborative efforts provide the best framework to disrupt the infrastructure of the Mexican-based drug trafficking organizations that deal in illegal drugs, murder, kidnapping, and extortion.

Just last week, an investigation by the FBI Hybrid squad in San Diego and multi-agency San Diego Cross Border Violence Task Force resulted in federal racketeering charges against 43 individuals from Southern California and Mexico who were associates of the Fernando Sanchez Organization, an offshoot of the Arellano Felix cartel. The President's FY 2010 Southwest Border Supplemental request called for the creation of five additional Hybrid Squads on the Southwest border.

4. Can you discuss the concept of hybrid teams and how they will be deployed across the southern border?

Response:

The FBI created Hybrid Squads in 2010 to address the violent crimes being committed by gangs and organized criminal enterprises. The Hybrid Squads co-locate FBI Agents who have significant experience investigating violent crimes with Agents experienced in conducting gang/criminal enterprise investigations. These squads investigate individual violent crimes and use collected intelligence to determine the structure and leadership of the gang/criminal enterprise involved and to disrupt and dismantle it.

Two of the first three Hybrid Squads were placed in SWB field offices (San Diego and Phoenix) and the third was placed in Philadelphia. The San Diego Cross Border Violence Task Force recently became co-located with and integrated into the existing OCDETF Co-located Strike Force in San Diego. The Administration's Fiscal Year (FY) 2010 SWB Supplemental provides funding and personnel to enable the FBI to create additional Hybrid Squads on the SWB.

5. What is the timeline for deploying these new resources?

Response:

The FBI intends to establish additional Hybrid Squads with the funding and personnel included in the FY 2010 Supplemental. The FBI received this authority in September 2010 and plans to have new hybrid squads operational by the spring of 2011.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.005

Mortgage Fraud

When you were last before the Committee in March 2009, you testified that the FBI's mortgage fraud caseload has more than doubled in the past three years, and the surge shows no sign of subsiding. You also stated that the additional cases are straining the agency's resources. At that time, I asked you to look into whether or not the FBI had decreased the number of agents working on mortgage fraud cases in California. Last month, the Department of Justice announced the results of a nationwide takedown known as "Operation Stolen Dreams."

6. How many agents does the FBI have in California working on mortgage fraud? Do you expect additional arrests and prosecutions as a result of "Operation Stolen Dreams"?

Response:

Currently, 54 FBI Agents are addressing mortgage fraud in California. As of 7/31/10, these Agents were investigating 423 pending mortgage fraud cases and had contributed to 220 informations and indictments and 106 convictions in FY 2010.

Operation Stolen Dreams was the second initiative to address mortgage fraud as a nation-wide take down, following the 2008 mortgage fraud initiative called Operation Malicious Mortgage. The FBI expects Operation Stolen Dreams to generate additional investigations, arrests, and prosecutions, in part as the result of guilty pleas pursuant to which subjects provide information regarding others involved in these activities.

7. Is the mortgage fraud caseload still increasing? What additional measures have you taken to ensure that the FBI has the agents to combat this growing problem?

Response:

The mortgage fraud caseload is still increasing. At the end of FY 2009, the FBI had received 67,190 Suspicious Activity Reports (SARs) and had a pending mortgage fraud caseload of 2,794 cases. By July of FY 2010, the FBI had received 58,640 SARs during the FY and was investigating 3,030 cases.

To ensure FBI Agents are able to address this caseload, the FBI has implemented a risk-based model for identifying the field offices with the greatest need and is allocating greater resources to these offices to address this crime problem.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.006

Priority is given to those field offices where the greatest impact from additional resources can be realized, as determined with the benefit of information obtained from our law enforcement partners and industry and regulatory professionals. The FBI also leverages these relationships to maximize the impact of our investigative resources, participating in 23 mortgage fraud task forces and 67 mortgage fraud working groups.

8. Has the FBI identified systemic problems in the mortgage market and, if so, is the Department of Justice prepared to share their views with the Senate on what additional legislation needs to be enacted to prevent such massive mortgage fraud in the future?

Response:

The FBI is responsible for investigating criminal violations of Federal laws. As a law enforcement agency, rather than a regulatory agency, the FBI does not have the expertise, nor is it part of our mission, to identify possible systemic problems in the private sector. The FBI believes this question would be more appropriately posed to those individuals or agencies that possess subject matter expertise.

The FBI works closely with its partners in the Department of Housing and Urban Development (HUD), including HUD's Office of the Inspector General (OIG), and at the Federal Housing Administration to identify potential fraud risks, particularly in regard to housing incentive programs and other economic stabilization efforts.

The FBI will be pleased to work with appropriate regulatory agencies, the Department of Justice (DOJ), the Office of Management and Budget (OMB), and the Congress to identify legislation that might help to prevent such extensive mortgage fraud in the future.

Guns- MAIG Recommendations

There are deep divisions in the Congress about issues relating to safe regulation of firearms. However, all sides, at least publicly, say we should better enforce the laws that are already on the books. So along those lines, almost a year ago, on August 7, 2009, the organization Mayors Against Illegal Guns provided a *Blueprint* to the Department of Justice that outlined 40 recommendations to better enforce existing gun laws. I have asked the Attorney General about this before, and have been told repeatedly that DOJ is reviewing the report. I am still waiting for the outcome of this review.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.007

Let me ask you about one particular area that is the subject of one of these recommendations. I am concerned about the apparent lack of enforcement against prohibited purchasers who illegally try to buy guns from legitimate dealers. These purchasers who fail a National Instant Criminal Background Check System (NICS) check almost certainly have committed a federal felony by falsely certifying on background check Form 4473 that they were not a prohibited purchaser. I understand that very few of these cases are pursued: in 2005, the FBI referred 67,713 such cases to ATF, but U.S. Attorneys only prosecuted 135 of them. To determine which cases to prosecute, the *Blueprint* recommends that DOJ develop a national risk assessment tool to identify factors most associated with risk of subsequent illegal activity.

9. Has the Justice Department or the FBI studied whether people who are rejected by NICS subsequently commit violent crimes, and/or identified the factors most associated with the risk of subsequent illegal activity? If so, when was the study completed and what were the results? If no such study has been undertaken, would the FBI consider doing one?

Response:

The FBI has not studied whether people who are denied the transfer of a firearm by the National Instant Criminal Background Check System (NICS) subsequently commit violent crimes, and we have not used NICS information to identify the factors most associated with the risk of subsequent illegal activity. If requested, the FBI would consider conducting, or would support another authorized organization in conducting, such a study within any legal limitations.

Hawalas

As you know, Al Qaeda has financed some attempted terrorist attacks through the use of the informal hawala money exchange system. All money service businesses - including hawaladars - must register with the Treasury Department. Registration requires the applicant to provide: contact information, a government-issued identification number, and a primary transaction account. State licensing requirements often also must be fulfilled.

10. In your opinion, are these registration requirements sufficient to provide the FBI with the information it needs in potential counterterrorism investigations? What additional resources are needed by the FBI to track illegal money transfers to potential terrorists?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.008

Registration requirements applicable to Money Service Businesses (MSBs) are imposed both by the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and by some states. Often, the registration requirements imposed at the state level are more restrictive and more easily enforced than those imposed at the Federal level. While the registration requirements, themselves, generally satisfy the FBI's investigative needs, the FBI's counterterrorism financing investigations would benefit from increased scrutiny of registered MSBs by both Federal and state regulators.

MSBs are required to capture customers'/senders' personal identification information, but there is no standardization as to what information is collected, how this information is collected, or how the information is maintained. The accepted forms of identification include drivers' licenses, passports, identification cards, and phone numbers. In addition, greater standardization in how MSBs record and license "authorized agents" and "authorized delegates" would allow the FBI to more quickly identify parent MSBs and their affiliates. Currently, MSBs' agents and delegates are permitted to operate in multiple states under the same MSB license, and MSBs are not required to maintain current listings of their agents and delegates or to routinely provide these lists to state and Federal regulators.

11. a. Is the FBI receiving information and intelligence from the Treasury Department on hawaladars?

Response:

The FBI receives information regarding hawaladars from the Department of the Treasury, including from FinCEN, both through regular liaison with these organizations and through our direct computer access to Bank Secrecy Act data. The liaison relationships between the Treasury Department and the FBI are cross programmatic, including both the FBI's Counterterrorism and Criminal Investigative divisions, which helps to ensure a timely exchange of relevant information and intelligence. For example, the FBI's Terrorist Financing Operations Section (TFOS) is working with the Treasury Department regarding the possible targeting and exploitation of Somali MSBs. TFOS is also working with FinCEN's MSB Audit Unit to facilitate a more frequent and productive exchange of information.

b. Who has the primary responsibility for tracking money going in and out of the country?

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.009

Response:

The Department of the Treasury, including FinCEN, and state governments are responsible for tracking money moving into and out of the country. MSBs are required to obtain state licenses and to abide by state laws and regulations.

Several FBI field offices have conducted investigations that have either involved hawalas or produced intelligence products regarding their use. In these cases, efforts are made to share the information or intelligence both regionally and nationally.

Questions Posed by Senator Feingold

12. Officers and employees of Blackwater Worldwide, now known as Xe Services, are currently the subject of three criminal indictments for separate incidents, including murder charges in Afghanistan. Federal regulations authorize the suspension or debarment of contractors that demonstrate a lack of business integrity or honesty. Do you think it would be a good policy for the U.S. government to conduct thorough investigations of any company whose employees have been indicted for multiple criminal violations to determine if they lack business integrity before deciding to award that company another government contract?

Response:

Pursuant to the Attorney General's Domestic Guidelines for FBI Operations, any investigation must have an appropriate predicate such as allegations, reports, or facts or circumstances indicative of possible criminal activity or activity that threatens national security. The mere fact that one or more employees of a company have been indicted does not, in and of itself, constitute appropriate predication for investigation of the company. If, though, there are facts and circumstances indicating that the company, itself, endorsed or directed wrongdoing on the part of its employees, or otherwise engaged in illegal activity, investigation of the company would be appropriate. The FBI certainly agrees that the U.S. Government should investigate companies, including potential contractors, when the appropriate predicate for an investigation has been established.

13. How many other companies that have been indicted or convicted of a federal crime related to fraud, corruption, bribery, or embezzlement are still receiving government

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.010

contracts? Please specify the names of the companies, the current disposition of the case(s), and whether these case(s) involved charges against the employees and/or the corporation.

Response:

The FBI does not track this information because, as explained in response to Question 14, below, there is a government-wide list of suspended and debarred contractors that agencies reference before awarding a contract.

The FBI is, though, very concerned about fraud in government contracting, and we have taken proactive measures to address it. For example, the FBI's International Corruption Unit (ICU) hosts the International Contract Corruption Task Force (ICCTF), a partnership of nine Federal law enforcement agencies the mission of which is to investigate fraud and corruption related to the expenditure of U.S. taxpayer funds overseas. The FBI's ICU and the DOJ Fraud Section maintain certain statistical data concerning investigations conducted by the ICCTF, including such items as arrests, indictments, fines, and forfeitures. As an entity, the ICCTF has charged over 120 individuals, including government contractors, military officers, enlisted military personnel, and several companies.

14. How do you think we can better ensure that U.S. taxpayer dollars are not going to companies that engage in criminal activity or tolerate a culture of fraud and dishonesty? Do you have any suggestions for how we could better facilitate coordination between the FBI and suspension and debarment officers in other federal agencies?

Response:

Before awarding a contract to a firm that may have been involved in criminal activity, agencies review the Excluded Parties List System (EPLS) (www.epls.gov) online. This website includes information provided by prosecutors and courts when a conviction is obtained, offering a single consolidated list of firms that are ineligible to receive government contracts.

15. The State Department is soliciting bids for a $30 billion contract to train foreign prosecutors and law enforcement officials. Do you think that more of this type of work should be handled by the FBI and other officials at the Department of Justice, rather than outsourced to private corporations?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.011

Yes, and the Department of State is of the same view. In its Quadrennial Diplomacy and Development Review (QDDR), which was issued in December 2010, the State Department stated as follows.

> State will enter into interagency agreements . . . to draw on the skills, expertise and personnel of other federal agencies before turning to private contractors where State determines that building in-house government capability or promoting bilateral working relationships furthers our foreign policy priorities. For certain core functions, State will also establish a presumption to enter into agreements to draw on other agencies . . . to implement State programs overseas. In particular, given the national security implications of security sector assistance, State will look first to the Department of Justice, the Department of Defense, and the Department of Homeland Security to implement State programs involving counterterrorism capacity building, foreign law enforcement, or strengthening justice and interior ministries.

QDDR at p. 33 (emphasis added).

In accordance with the QDDR, we expect that the award of any contract to train foreign security sector institutions – including police officers and prosecutors – would be on a "demand" or "needs" basis, and therefore would not be called into play unless the Departments of Justice, Defense, and Homeland Security were unable to provide the capacity-building programs in question.

In this regard, we note that, with past State Department funding and support, DOJ has engaged in highly productive overseas capacity building, both through the Department's law enforcement agencies (the FBI, Drug Enforcement Administration, U.S. Marshals Service, and Bureau of Alcohol, Tobacco, Firearms, and Explosives) and through DOJ offices dedicated to building foreign capacity (the Office of Overseas Prosecutorial Development, Assistance, and Training, which works to build prosecutorial, criminal justice, judicial, and legislative capacity, and the International Criminal Investigative Training Assistance Program, which is responsible for building police and corrections capacity). DOJ institutional development and training programs build the

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.012

capability and capacity of host nations not only to fight domestic crime and threats but also to serve as full partners to both the United States and other nations in the global pursuit of terrorist groups, transnational organized crime, narcotics crime, international financial and commercial fraud, trafficking in persons, cyber crime, and other criminal enterprises. Because the success of this global pursuit is critical to the security of both the United States and these partners, it is important that it be accomplished by those best qualified to conduct it, as articulated in the QDDR. In addition, the use of contractors to conduct this training would deprive the FBI and other federal entities of the opportunity to enhance liaison, develop partnerships, and gather crucial information before there is a crisis. As the lead counterterrorism agency for the U.S., the FBI is often invited to respond to terrorism incidents overseas, where we work with the host nation's investigators. Those investigators must receive training that will help them not only conduct thorough investigations, but conduct them in such a manner that the results can be used by the FBI to garner additional intelligence and can be used in U.S. Federal courts in appropriate cases.

16. Do you think a company that has pled guilty to a crime under the Foreign Corrupt Practices Act or another related corruption charge should ever be eligible to train prosecutors or law enforcement officials overseas?

Response:

While this is not the FBI's decision, typically a company that has pled guilty to corruption charges would not have the necessary credibility to train prosecutors and law enforcement officials.

17. The FBI has shown tremendous initiative by building the Joint Operations Center of the International Contract Corruption Task Force and promoting inter-agency cooperation and coordination, but more needs to be done. What is the FBI's plan to expand its investigation of international fraud and corruption beyond Iraq, Afghanistan, and Kuwait?

Response:

The FBI appreciates the Senator's support for the work of the ICCTF, which is hosted by the FBI and includes the Joint Operations Center (JOC). The nine ICCTF partner agencies agree that the ICCTF model currently used in Kuwait, Iraq, and Afghanistan should be used at other locations around the world where U.S. assets are potentially at risk of fraud and corruption. Near-term expansion of

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.013

the ICCTF is planned in Pakistan and the Republic of Korea (ROK) and subsequent expansion of the ICCTF is being considered for locations in Haiti, Africa, and elsewhere. In support of the ICCTF's near-term expansion, the FBI anticipates deploying one Agent to the ROK and one Agent to Pakistan

It is the FBI's understanding that the Department of Defense Yongsan Relocation Program and Land Partnership Plan will involve the relocation of nearly all U.S. military personnel and equipment currently located between the ROK's Demilitarized Zone and Seoul to Camp Humphreys (an Army installation approximately 55 miles south of Seoul), which will triple in size. The construction and service contracts necessary to decommission some posts and augment others represent a significant opportunity for fraud and corruption. In order to assess the potential for fraud and corruption, and to develop an effective strategy for investigating it, one FBI Agent will be deployed to the ROK pursuant to the ICCTF mission.

In Pakistan, the U.S. Agency for International Development (USAID) is expending funds pursuant to the Enhanced Partnership with Pakistan Act of 2009, including in the Federally Administered Tribal Areas (FATA), which is generally recognized as the locus of significant insurgent activity. The threat of corruption and fraud concerning USAID funds is assessed as high, with the possibility that stolen funds may be diverted to insurgent causes, particularly in the FATA region. The USAID OIG has authorized two Agents and one host-nation investigator to work at the U.S. Embassy in Islamabad, and the FBI will deploy one Agent to work jointly with USAID-OIG investigators on behalf of the ICCTF. As U.S. Government spending continues in Pakistan, the FBI will continue to evaluate vulnerabilities to fraud and corruption and will adjust staffing accordingly.

In addition to the ICCTF's ongoing work in Iraq, Afghanistan, and Kuwait and the pending deployments to the ROK and Pakistan, the FBI continues to actively coordinate with its ICCTF partners, foreign law enforcement, non-governmental organizations, and regional liaison contacts to identify emerging vulnerabilities to fraud and corruption globally. The FBI and ICCTF are working proactively to identify and address international corruption and fraud involving U.S. interests. Although the ICCTF is an unfunded entity, the ICCTF partner agencies agree that the ICCTF model is the appropriate mechanism for addressing these matters.

18. Last week's Washington Post series on the Intelligence Community indicated that contractors make up somewhere around 30 percent of the top-secret workforce - and it suggests that they often cost more than hiring employees to do the same job. What

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.014

percentage of the FBI's intelligence personnel is made up of contractors? Has the FBI analyzed whether these contractors cost the FBI more than employees would? What benefit does the use of contractors provide?

Response:

The use of contractors, rather than recruiting new permanent employees, is appropriate in several circumstances. For example, when the need is only temporary or is part of a "surge" that will be of limited duration, such as the need for translation of a foreign language that is rarely encountered but critical to an investigation, the use of contractors is preferable to the recruitment of permanent employees who will not be needed in the long term. In addition, a surge or other emergency response may require the very quick acquisition of a particular skill set, and this quick response is not possible through the ordinary recruitment and hiring process. In other cases, the need may be for a specialized skill set that is not recognized by, and cannot be adequately compensated under, the General Schedule governing pay, such as a physicist fluent in Chinese.

A cost comparison cannot address these reasons for preferring contractors to permanent employees in appropriate cases, and making such a cost comparison would be extremely complex. The FBI has plans to review our contractor acquisitions to determine whether it would be appropriate to convert certain of these to permanent Federal employee positions.

19. Federal regulations prohibit the Bureau and other agencies from using contractors to conduct criminal investigations. What policies does the FBI have in place to ensure that government contractors, who could work for companies that are potentially the subject of an investigation, do not have access to sensitive information concerning ongoing criminal investigations?

Response:

Since the creation of the Automated Case Support system, the FBI's investigative case files have been maintained and accessed electronically. While the relatively rare access to paper files would be conducted in person, with ample opportunity for the file custodian to verify the propriety of a recipient's access to the file, electronic access to FBI files of all types, including investigative files, has been the subject of recent FBI policy.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.015

This policy specifies that the authorities and processes used to validate and grant access to FBI Information Systems (IS) are to be established in the System Security Plan for each IS. While these authorities and processes are different for each IS, they all require that a user possess a security clearance equal to or higher than the highest classification level of the information processed by the IS. System owners are responsible for ensuring that the processes used to grant access to the systems under their purview validate the user's security clearance and need to know the information the user will access. This applies to all users, including FBI employees, detailees, task force members, and contractors.

20. In the fall of 2009, FBI officials indicated they were very close to issuing new privacy guidance for the use of National Security Letters. Has that guidance been finalized and issued? If so, please provide a copy. If not, please indicate when it will be completed.

Response:

The Attorney General has approved procedures that will govern the FBI's handling of information derived from National Security Letters. We will provide these procedures to the Committee in its oversight capacity.

21. Please provide the Committee with an unredacted copy of the FBI's Domestic Investigations and Operations Guide (DIOG). The DIOG is an unclassified/FOUO document, yet when Senator Leahy asked the Department of Justice for a copy of it in November 2009, he was told the Committee would be provided only "an opportunity to view the redacted portions." The DIOG is hundreds of pages long, and the Committee cannot effectively conduct oversight with only occasional, short term access to the document. If the FBI or Department of Justice have security concerns, security arrangements can be made, just as they are made with the many classified documents that the Committee receives regularly from the executive branch.

Response:

On 9/2/10, the FBI hand delivered copies of the unredacted Domestic Investigations and Operations Guide (DIOG) to the Security offices of both the House and the Senate.

22. When the FBI seeks access to GPS data to track a person in a criminal investigation, does it obtain a search warrant?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.016

Absent consent, policy requires the FBI to obtain a warrant based upon a showing of probable cause to compel a wireless provider to disclose ongoing GPS (or similarly precise) location information.

23. In each of 2007, 2008 and 2009, how many times has the FBI obtained access to GPS data in the course of a criminal investigation? Please provide a separate response for each of the three years.

Response:

Prior to FY 2010, the FBI did not keep statistics on the number of times GPS (or similarly precise) location information was used in investigations. In FY 2010, the FBI created a form to document the acquisition of cellular technology information in our investigations. This will enhance the FBI's ability to report this information in the future.

24. In each of 2007, 2008 and 2009, how many times did the FBI obtain the contents of email communications in a criminal investigation without satisfying a probable cause standard, such as by using an order under 18 U.S.C. § 2703(d) or an administrative subpoena? In how many of those instances was notice delayed pursuant to 18 U.S.C. § 2705? Please provide a separate response for each of the three years.

Response:

The FBI only collects statistics regarding the disclosure of communications made pursuant to emergency disclosure provisions (18 U.S.C. § 2702(b)(8)). These statistics are collected by the FBI in order to fulfill its statutory obligation annually to report these disclosures to Congress. That annual report, entitled "Voluntary Disclosures Pursuant to 18 U.S.C. § 2702(b)(8) Component Report," is provided to the Judiciary Committees of both the House and Senate. Annual reports covering the years 2007-2009 have been made to Congress and include disclosures made in both criminal and terrorism cases. The total number of disclosures documented in those reports is not limited to email communications, but instead includes disclosures of content in any form, including text messages and stored communications.

The FBI does not maintain records from which statistics could readily or accurately be derived regarding the number of times email content has been received in the other circumstances authorized by law. Likewise, there are no

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.017

records from which statistics could readily or accurately be derived regarding the number of times delayed notice has been authorized under 18 U.S.C. § 2705.

Questions Posed by Senator Durbin

Sentinel Computer System

25. Director Mueller, we have spoken on a number of occasions about my concerns with the delays and cost overruns in setting up the FBI's Sentinel online case management system. The Justice Department OIG has also raised serious concerns in its March 2010 report on the progress being made with the four phases of the Sentinel project. The OIG report identified four major factors that led to schedule delays and increased costs with implementation of Phase 2 of Sentinel: (1) problems with Sentinel's electronic forms, (2) performance and usability issues, (3) integration issues with Sentinel and the former network security features, and (4) software code inefficiencies.

a. What is the FBI doing to ensure that similar problems do not plague Phase 3 and Phase 4?

Response:

The FBI is consulting with industry experts to evaluate how best to complete the Sentinel application. We are evaluating the options with the benefit of the lessons learned from Phases 1 and 2 and the identified "best practices." The FBI will be pleased to brief the Committee regarding our plan forward once it is finalized.

b. Have the FBI and Lockheed Martin agreed on a revised budget and schedule for Phases 3 and 4?

Response:

The FBI and Lockheed Martin have engaged in discussions regarding a variety of options on how best to move forward. During the "stop work" period, the FBI is also looking at alternatives to the engineering development effort. Until we determine the path forward, no revised budget or schedule are available.

c. Is the FBI considering opting out of the contract with Lockheed Martin for Phases 3 and 4?

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.018

Response:

During the "stop work" period, all options are being considered. These options include continuing with Lockheed Martin under the current contract approach, changing the contract type, or changing the development approach. We are also considering a revision of responsibilities related to the development process, which may affect Lockheed Martin's role. The phased approach to contract execution, along with the stop work order, have allowed the FBI to take the time to conduct its due diligence review before authorizing further performance.

26. The OIG expressed concern in its 2009 Audit Report that Lockheed Martin had not provided or had reported incorrect information under the Sentinel Measurement Plan - a plan designed to track Sentinel's monthly development. What is the FBI doing to guarantee that in the future Lockheed Martin provides timely and accurate information in these vital reports?

Response:

The FBI agreed with the concern expressed by the OIG in its 2009 Audit Report. Although Lockheed Martin reported System Performance Measurements in accordance with the Measurement Plan V5.0, dated 7/28/09, not all performance measurements provided value because of the short time between reporting periods. To address this, the Sentinel Program Management Office instituted daily and weekly reporting of various measures to identify and resolve program issues as quickly as possible.

27. The OIG has expressed concern with the FBI's internal reporting on Sentinel's progress.

a. Why did the FBI switch from a monthly to a quarterly Program Health Assessment, and what is the FBI's response to the OIG's recommendation that the FBI reinstitute monthly reports?

Response:

The Program Health Assessments (PHAs) compare actual delivery to planned delivery. The PHAs were performed on a monthly basis beginning with Phase 2, but were suspended on 10/16/09 when Sentinel entered into a "breach" condition for Segment 2 of Phase 2. One of the factors being considered in developing the plan for moving forward is the ability to measure progress frequently. Any future

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.019

plans will include reporting mechanisms that are tailored to ensure appropriate transparency and frequency.

b. As of March 2010 the DOJ's Investment Review Board had not received a Sentinel status update in 6 months. Has there been an update? If not, please explain why.

Response:

The Sentinel Program Management Office provided a thorough update to the DOJ Investment Review Board (DIRB) in August 2010, and in October 2010 the FBI received certification on Sentinel from the DIRB.

Questions Posed by Senator Whitehouse

28. Reports indicate that the overwhelming majority of cyber crime is preventable by the use of simple commercial off-the-shelf technology and common sense. Is this consistent with the experience of the FBI in its investigative activities in the area of cyber crime?

Response:

In the FBI's experience, many individual and business computer users routinely fail to employ computer security "best practices," neglecting to keep their security suites, operating systems, and applications patched and updated and failing to turn on and routinely audit their intrusion detection and network logging features. Criminal enterprises and foreign intelligence services are constantly evolving, developing ever-more sophisticated tools and means of infecting computers. Consequently, the technology that combats malware, spyware, viruses, and other cyber crime is typically reactive, trying to catch up to the crime. This leaves the consumer vulnerable from the time when malicious code is created to the time when the combative technology is updated.

While the systematic use of commercial off-the-shelf technology combined with common sense can reduce some types of cyber crime, there is no off-the-shelf tool that is able to prevent all malware, spyware, and viruses. There is also no technological defense against insiders who abuse their authorized access or who are manipulated into providing data access to others. Additionally, because new malware is created almost daily, consumer-purchased technology must be updated just as frequently to remain effective. While some behaviors and tools can help protect against cyber invasions, we know of nothing that can prevent the

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.020

overwhelming majority of cyber crime. While we can do a better job of making our systems intrusion-resistant, they will not be intrusion-proof. Practicing better cyber hygiene would reduce security risks substantially.

29. On July 20, 2010, *The Boston Globe* reported that Kexue Huang had been charged with "12 counts of economic espionage to benefit a foreign government." An affidavit in support of arrest filed in the District of Massachusetts indicates that these charges included alleged violations of 18 U.S.C. § 1831. The article in *The Boston Globe* indicates that only six or seven individuals ever have been charged with economic espionage to benefit a foreign government or instrumentality. Are these figures correct and do they indicate that better statutory tools are needed to facilitate the prosecution of economic espionage to benefit foreign governments?

Response:

The Economic Espionage Act of 1996 (EEA) criminalizes certain acts, including the wrongful appropriation of trade secrets, when they are accomplished "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent." (18 U.S.C. § 1831(a)(1).) Since the EEA was enacted, economic espionage has been charged on seven occasions against a total of ten individuals. These figures are not unusually low in light of the relatively recent enactment of the statute. Historically, it has taken some time for both the FBI and DOJ to fully use a new prosecutorial tool. The FBI does not interpret these figures as indicating that better statutory tools are needed. We have seen an increase in the use of 18 U.S.C. § 1831 during the period since enactment and, while this provides only an indirect indication that the statute is sufficient as written, we are aware of no information indicating the contrary.

Conclusively demonstrating that a trade secret theft was intended to benefit a foreign government or instrumentality can pose significant challenges. 18 U.S.C. § 1832, which more broadly criminalizes the theft of trade secrets for the economic benefit of anyone other than the owner thereof, is charged more frequently than violation of § 1831, including cases in which a theft may be linked to a foreign government or instrumentality but this link is difficult to prove.

The FBI will continue to work closely with DOJ to ensure that all offenses meeting the statutory threshold are appropriately investigated and prosecuted.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.021

30. Please provide a deployment diagram of the location and purpose of FBI cyber-protection resources. Please provide further detail than available in the report submitted to Congress in 2009 pursuant to the PRO-IP Act.

Response:

The FBI has proposed a briefing for staff regarding our deployment of cyber-protection resources.

Questions Posed by Senator Kaufman

31. In the aftermath of the savings and loan crisis, bank regulators helped the FBI and other law enforcement agencies with criminal referrals in the form of detailed narrative memos and extensive attachments. Have you been getting those sorts of referrals in connection with the most recent financial crisis?

Response:

The criminal referrals generated in the aftermath of the savings and loan crisis were replaced by SARs. SARs are electronically filed, do not support attachments, and are, by their nature, concisely written. The sort of information previously attached to criminal referrals is now referenced in the SARs and is available by request to the originating agency.

32. Are you encouraging bank regulators to make such referrals?

Response:

Although bank regulators, themselves, make very few referrals, SARs are issued by the financial institutions subject to that regulation in the ordinary course of business.

In FY 2010, the entities regulated by the below regulatory agencies submitted the following numbers of SARs.

Agency	Number of SARs
Office of the Comptroller of Currency	323,284
Federal Deposit Insurance Corporation	112,068

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.022

Office of Thrift Supervision	30,166
Federal Reserve Board	75,677
National Credit Union Association	56,295

33. What is the FBI doing to ensure that it takes full advantage of the regulators' expertise and knowledge of the relevant institutions in terms of identifying, investigating, and prosecuting financial fraud?

Response:

Members of the bank regulatory community routinely participate in numerous mortgage and bank fraud working groups throughout the country, the purpose of which is to share information and intelligence. These groups include the National Interagency Bank Fraud Enforcement Working Group and its recently formed subgroup, the Mortgage Fraud Working Group. In addition, individual financial institution fraud investigators maintain liaisons with bank regulatory personnel on case-specific matters. Members of regulatory agencies, including the Federal Deposit Insurance Corporation OIG, participate in fraud investigations when appropriate.

The FBI also participates in the President's Financial Fraud Enforcement Task Force, which coordinates efforts to investigate and prosecute financial fraud. This task force includes representatives from Federal agencies, regulatory authorities, OIGs, and state and local law enforcement who collectively bring to bear a powerful array of criminal and civil enforcement resources. With this breadth of perspective and resources, the task force is able to investigate and prosecute significant financial crimes and combat discrimination in the lending and financial markets.

The FBI continues to expand its liaison contacts and cooperative efforts with regulatory agencies. For example, in addition to its task forces, working groups, liaison contacts, and other channels of communication, the FBI is embedding an Agent with the Securities and Exchange Commission (SEC) at their Washington, D.C., headquarters. This Agent will be responsible for coordinating intelligence and handling referrals to and from the SEC. The FBI believes this cooperation and other efforts like it will allow the FBI to better leverage the regulators' expertise and knowledge.

Questions Posed by Senator Franken

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.023

34. According to an FBI press release dated June 17, 2010, 1,215 criminal mortgage fraud defendants have been responsible for approximately $2.3 billion in losses since March 1, 2010, and approximately $10.7 million of this has been recovered through criminal prosecutions. Additionally, 191 civil enforcement actions have resulted in recovery of $147 million. Please explain why criminal enforcement has resulted in seizure of only $10.7 million of a total of $2.3 billion lost, and what barriers the FBI faces in restoring victims of mortgage fraud schemes.

Response:

Most Federal courts have held that forfeiture law permits only the pre-trial seizure of assets that represent proceeds of the defendants' crimes or are directly traceable to those crimes. It is often difficult to trace a defendant's funds to an underlying crime, particularly in light of the sophisticated money laundering techniques used by white collar criminals. Criminal forfeiture is not effective against a defendant who has already laundered the proceeds of the crime into the hands of third parties. Once convicted, though, prosecutors can seek a criminal forfeiture money judgment equal to the total amount of criminal proceeds generated, which allows law enforcement to seize the defendant's assets without the need to trace those assets to criminal activity. A third party who has acquired an actual ownership interest in assets traceable to the crime can additionally be pursued through civil forfeiture, which usually takes place after arrest and is often stayed by the courts until the related criminal proceedings have concluded.

When the mortgage fraud victim is a financial institution or state-regulated mortgage lender, any recovered funds may be returned to the Federal Deposit Insurance Corporation, the National Credit Union Administration, or the bankruptcy trustee, depending on the circumstances. As with other forfeitures, there are likely to be practical problems in actually obtaining any funds that are forfeited.

As the question recognizes, in addition to the $10.7 million seized under Federal forfeiture authority during Operation Stolen Dreams, another $147 million was seized by civil authorities. This was possible because these civil authorities have broader authority to seize assets than the authority afforded law enforcement agencies under Federal forfeiture law.

35. Please describe the process by which the FBI chooses to prioritize resources for investigation of mortgage fraud cases.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.024

Response:

The FBI prioritizes cases according to the anticipated impact of our investigation, seeking to address the most prolific schemes with the greatest impact on the communities in which the fraud occurs. This prioritization also takes into account the ability of the local U.S. Attorney's Office (USAO) to prosecute the case. Currently, approximately 70 percent of the FBI's pending mortgage fraud cases involve losses of over $1 million.

36. What measures are the FBI taking to ensure that criminal background information released to employers contains up-to-date arrest and disposition information?

Response:

The FBI takes a proactive approach to ensuring that information contained in and available through its systems, including criminal history record information (CHRI), is current and accurate. For example, the Integrated Automated Fingerprint Identification System allows criminal justice and law enforcement agencies to submit fingerprint-based criminal history information electronically, and this information is immediately available for authorized noncriminal justice purposes, such as licensing and employment checks. Another example of this effort is the FBI-managed National Fingerprint File (NFF). In recognition of the reality that state rap sheets are often more complete than the information submitted for inclusion in FBI systems, the NFF reaches out to obtain state rap sheets and provides them to requesting agencies.

Among the greatest challenges in this area is ensuring the timely inclusion of disposition information, because an arrest may result in anything from no further action to felony conviction and incarceration. The FBI conducts continual liaison with the criminal justice and law enforcement agencies that voluntarily submit CHRI to advocate the timely submission of dispositions and other CHRI into FBI systems so it is readily available for law enforcement, national security, and noncriminal justice purposes. An FBI unit that specializes in processing dispositions submitted through various channels by state and Federal agencies processed nearly 900,000 dispositions in FY 2009. Another FBI team assists individuals who believe inaccurate or incomplete information is contained in their FBI identification records. This team reviews each request to identify the information in question and works with external agencies to obtain and update the information to the greatest extent possible.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.025

The FBI has developed several ways to increase the disposition submission rate and has initiated several means of improving the flow of CHRI, including dispositions. A recent example is the Disposition Message Key, which allows agencies to update disposition information electronically rather than through a manual paper process. Another example occurs in the context of the FBI's National Instant Criminal Background Check System (NICS), which conducts background checks on individuals purchasing firearms. Pursuant to a NICS check, the FBI obtains dispositions and other CHRI that is missing from arrest records by contacting the appropriate court or arresting agency, using the CHRI to update records in appropriate cases.

The FBI also manages internal and external task forces and working groups that focus on CHRI improvement. These groups vary in strategy and focus, but share the common goal of improving the accuracy and thoroughness of the information available to the end users of FBI criminal justice information systems. Two of these task forces work actively with external agencies. The membership of one of these task forces includes representatives from state repositories, the National Center for State Courts, the Bureau of Justice Statistics, the Office of Personnel Management, several state supreme courts, and various related agencies. The other task force organizes an annual conference during which representatives from throughout the criminal justice community attend classes and workshops and collaborate regarding ways to improve information reporting within their agencies.

37. Does the FBI keep data on where incidents of human trafficking occur? If so, how many human trafficking cases occurred on or near Indian reservations in 2009? How many human trafficking cases occurred elsewhere during the same period?

Response:

While the FBI does not specifically track this type of data, the FBI's Indian Country Special Crimes Unit is not aware of any human trafficking investigations on Indian reservations in FY 2009. The FBI is, though, currently investigating two child prostitution cases involving Native Americans in the northern plains region.

During FY 2009, the FBI opened 175 new Human Trafficking investigations, with a total of 305 Human Trafficking cases open at the end of FY 2009. "Human Trafficking" investigations include cases involving forced labor,

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.026

domestic servitude, sex trafficking of adults, and sex trafficking of non-citizen victims.

38. Please describe the nature of the services provided by the FBI's Victim Specialists in Indian Country.

Response:

The following services are consistent with the Victims of Crime Act and can be provided to victims and their families by FBI Victim Specialists.

Services Associated with Mandatory Requirements

- Helping case Agents to identify victims and uploading FD919 forms
- Providing written and oral information to victims regarding their rights and available services
- Keeping victims informed of case status
- Relaying information to Agents from victims regarding threats they have received
- Services associated with investigative support
- Providing on-scene assistance to victims
- Accompanying Agents when they interview victims or deliver distressing news
- Explaining forensic identification issues (such as DNA testing, the autopsy process, and procedures for the return of victims' remains)
- Cleaning and returning property and personal effects to victims
- Returning property used as evidence to victims
- Maintaining contact with victims and alerting Agents to issues that could affect a victim's ability to cooperate
- Arranging forensic exams for victims of sexual and physical abuse
- Assisting with photographing injuries resulting from domestic violence
- Participating on Emergency Response Teams for the purpose of assessing needs and providing support to victims

Standard Services

- Providing crisis intervention
- Conducting assessments of victims' needs
- Conducting liaison with the FBI Headquarters (FBIHQ) Office for Victim Assistance (OVA) to obtain emergency victim assistance funds
- Explaining the criminal justice system to victims

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.027

• Providing information to victims regarding the impact of crime
• Making referrals for victim services, such as counseling and support groups, and assisting when problems with access are encountered
• Assisting victims with compensation applications and coordinating FBI verification of victimization for state compensation program officials
• Transporting/accompanying victims to case-related appointments
• Locating emergency housing, food, and clothing
• Conducting follow-up with vulnerable victims
• Managing the Victim Notification System
• Creating and maintaining an appropriate and victim-friendly space within the office
• Coordinating with the USAO Victim-Witness Coordinator to transition responsibilities following indictment

Special Services

• For child victims/witnesses, participating on multi-disciplinary teams
• For victims of sexual assault, arranging for HIV/STD testing and medical counseling sessions

Other Activities

• Maintaining regular contact and productive working relationships with USAO Victim-Witness Coordinators and peers in other Federal agencies
• Identifying tribal, local, and regional resources for victims
• Maintaining a manual of tribal, local, and state resources
• Maintaining regular contact with the state crime victim compensation program administrator or staff
• Participating in tribal, local, regional, and state victim assistance networks, councils, and advisory groups
• Pro-actively meeting with Squad and Unit supervisors to obtain feedback and solicit ideas for enhancing victim assistance efforts
• Providing annual office training regarding victim assistance requirements and resources
• Providing orientation to new Agents
• Checking frequently with Agents to ensure they are providing victim information
• Maintaining professional skills and knowledge through continuing education and training
• Providing the required activity and compliance report to the FBIHQ OVA

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.028

39. Approximately how many individuals does each Victim Specialist serve? Of which crimes are these individuals typically victims?

Response:

In the Victim Notification System, 650 victims were categorized as Native Americans in FY 2009. In that year, the FBI had 31 Indian Country Victim Specialists, so the ratio of newly identified victims to Victim Specialist was approximately 21 to 1.

The crimes of which these Native Americans were classified as victims includes the entire scope of criminal violations, including homicides, child physical and sexual assaults, violent assaults, drug and gang crimes, gaming violations, and property crimes.

Questions Posed by Senator Sessions

40. At our January 20th hearing to address the Christmas Day attempt to bomb Northwest Flight 253 in Detroit, I asked you who made the decision to treat Umar Farouk Abdulmutallab as a civilian criminal rather than as an unprivileged enemy belligerent. You responded: "The decision was made by the agents on the ground, the ones that took him from the plane, and the followed upon the arrest..."

a. Do you agree that the decision to treat a foreign terrorist as a civilian criminal defendant is a policy decision, just as it would be a policy decision to treat that foreign terrorist as an unlawful enemy belligerent under the laws of war?

Response:

Umar Farouk Abdulmutallab was arrested inside the United States. Both before and after the 9/11/01 attacks, the practice of the U.S. government has been to arrest and detain under Federal criminal law all terrorist suspects who are apprehended in the United States. In recent history, only two individuals have been apprehended in the United States and subsequently held under the law of war: Jose Padilla and Ali Al Marri. In both of these cases, the individuals were first arrested and held in the criminal justice system and were transferred to military custody under the law of war only after they were formally designated enemy combatants by the President. In both cases, the transfer to military custody raised serious statutory and constitutional questions in the courts. Both men were

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.029

later returned to the civilian criminal justice system and convicted. Thus, clearly the decision to treat an arrestee as an unlawful enemy belligerent raises important legal and constitutional questions.

b. Do you agree that field agents should not be put in the position of making policy decisions?

Response:

Field agents are not put in the position of making policy decisions. The FBI does not have the authority to hold an arrestee as an unprivileged enemy belligerent or to otherwise hold a person against his or her will outside of the criminal justice system. The FBI notifies other agencies when it intends to arrest an operational terrorism suspect in the United States. Notification informs other agencies that the suspect will be handled in accordance with the requirements of the criminal justice system. Notification also allows other agencies to propose any alternatives to the criminal justice system they think are or might be appropriate.

c. What is the F.B.I. doing - and what have you done since the Christmas Day incident - to create clear guidance so field level agents do not have to make this kind of decision on their own in the next terrorism case?

Response:

Please see the response to subpart b, above.

d. Since December, has the administration 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?

Response:

There is (and has been since well before December) extensive interagency cooperation and coordination regarding counterterrorism efforts, including on decisions related to the apprehension and detention of terrorists. Prompt notification of other agencies in the event of an arrest allows for high-level discussions of all options where warranted.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.030

e. When a foreign terrorist is arrested, what is more important - the goal of prosecution or the goal of gathering actionable intelligence?

Response:

Prosecution and the gathering of actionable intelligence are not mutually exclusive objectives. One of the most important reforms since 9/11/01 has been to more fully integrate the FBI into the Intelligence Community. The fact that the FBI retains its law enforcement authority does not alter its primary mission since 9/11/01 - to gather intelligence to protect and defend the United States against terrorist threats. The FBI has successfully obtained critical intelligence from terrorist suspects for many years. The criminal justice system has proven to be one of the most effective weapons available to our government for both incapacitating terrorists and collecting intelligence from them.

f. What is the administration doing to ensure that actionable intelligence is not lost when a terrorist is arrested?

Response:

Obtaining actionable intelligence is the FBI's highest priority. The FBI's longstanding approach to obtaining actionable intelligence from a terrorist or a 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.

g. We know that Umar Farouk Abdulmutallab was advised of his right to remain silent after 50 minutes of public safety questions. Did the F.B.I. advise Mr. Abdulmutallab that he had the right to consult the Nigerian consulate before being questioned?

Response:

On 12/25/09, Abdulmutallab was detained by U.S. Customs and Border Protection officers at the airport. No consular notification was attempted on that date. On 12/26/09, officials from the Nigerian Embassy appeared at the FBI's Detroit Office, having been alerted by the news media to the fact that Abdulmutallab was a Nigerian national and was in custody. Embassy officials

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.031

had access to Abdulmutallab the same day. The United States Attorney's Office was aware of the Nigerian Embassy's involvement and did not separately notify the consulate.

41. In a February 3, 2010 letter to Senator Mitch McConnell, Attorney General Eric Holder stated that "the consistent, well-known, lawful, and publicly-stated policy of the FBI has been to provide Miranda warnings prior to any custodial interrogation conducted inside the United States." This assertion appears to be correct, as the FBI's Domestic Investigations and Operations Guide (DIOG) states: "Within the United States, Miranda warnings are required to be given prior to custodial interviews if the subject is significantly restricted in his/her freedom of action to a degree normally associated with a formal arrest." Do you agree?

Response:

The FBI's longstanding policy has been to provide *Miranda* warnings before interviewing a person when that person's freedom of movement is restricted to a degree associated with formal arrest. The FBI's policy also recognizes that there are lawful exceptions to this rule, including when questions are reasonably prompted by an immediate concern for public safety or the safety of the arresting agents. In addition, FBI policy recognizes that there may be exceptional cases in which, although relevant public safety questions have been asked, agents nonetheless conclude that continued unwarned interrogation is necessary to collect valuable and timely intelligence not related to any immediate threat, and that the government's interest in obtaining this intelligence outweighs the disadvantages of proceeding with unwarned interrogation.

42. At last week's hearing, you testified concerning the High-Value Detainee Interrogation Group that, for an arrest of a terrorism suspect on U.S. soil, "it would be ourselves [the FBI], generally, that would conduct the interrogations." Assuming that an exception does not apply, would the FBI therefore be required, under the DIOG, to read a suspect his or her Miranda warnings prior to interrogation in such instances?

Response:

Agents should ask any and all questions that are reasonably prompted by an immediate concern for the safety of the public or the arresting agents without advising the arrestee of his *Miranda* rights. After all applicable public safety questions have been exhausted, agents should generally advise the arrestee of his *Miranda* rights and seek a waiver of those rights before any further interrogation

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.032

occurs. As indicated above, there may be exceptional cases in which, although relevant public safety questions have been asked, agents nonetheless conclude that continued unwarned interrogation is necessary to collect valuable and timely intelligence not related to any immediate threat, and that the government's interest in obtaining this intelligence outweighs the disadvantages of proceeding with unwarned interrogation. In all cases, the FBI's primary goal is to elicit information needed to secure the safety of the American people.

43. You testified that the FBI essentially takes an expansive view of the exception in New York v. Quarles, 467 U.S. 649 (1984), which justifies the delayed provision of Miranda warnings where there exists a threat to public safety. The case law concerning the applicability of Quarles to the terrorism setting (*e.g.*, questioning a suspect about known associates and future plots) is scant [at] best. Why is the Bureau comfortable using the Quarles exception in such circumstances - which would pose a risk of later suppression of statements and rule out the use of follow-up questioning if information provided has proven to be inaccurate upon further investigation - when the option of turning the interrogation over to an entity not covered by the DIOG is available?

Response:

Pursuant to the *Quarles* exception, FBI agents may ask questions that are reasonably prompted by an immediate concern for the safety of the public or the arresting agents without a *Miranda* warning, and the answers to such questions are admissible in Federal court. In light of the magnitude and complexity of the threat often posed by terrorist organizations, particularly international terrorist organizations, and the nature of their attacks, the circumstances surrounding an arrest of an operational terrorist may warrant significantly more extensive public safety interrogation without *Miranda* warnings than would be permissible in an ordinary criminal case. Experienced interrogators - across the law enforcement, intelligence, and defense communities - agree that successful interrogation does not depend on particular "techniques." Instead, successful interrogation depends on lawful interrogation strategies based on extensive knowledge of an arrestee and his organization. The FBI has successfully obtained critical intelligence from terrorist suspects for many years using such strategies.

44. At the hearing, we discussed the decline of FBI enforcement in fraud cases. I referenced the numbers from the 2008 report of the Administrative Office of the U.S. Courts (AO), which provided criminal case filings in traditional FBI enforcement areas. You expressed doubt in the hearing that those were the correct numbers.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.033

a. Do you believe that the fraud, bank larceny, and related case filings numbers we discussed are underrepresented in the AO's report? If so, why?

Response:

While the FBI is not able to comment on the accuracy of statistics provided by the Administrative Office of the U.S. Courts (AOUSC), we note that variations in recording systems can create apparent disparities. For example, the AOUSC uses the general classification of "property offenses," with sub-classifications of: 1) burglary, larceny, and theft; 2) embezzlement; 3) fraud, forgery, and counterfeiting; and 4) other. Because these classifications do not correspond directly to classifications used by the FBI, it is difficult to make correlations between the two sets of statistics.

Following the attacks of 9/11/01, the FBI implemented strategies that direct our resources toward threat-based, intelligence-driven investigations. In line with these efforts, we have used our expanded and maturing intelligence collection and analysis capabilities to better identify and understand the growing threat posed by financial frauds, strategically shifting our investigative resources away from lower priority matters to address the more complex and long-term investigations.

An example of this re-prioritization can be seen in our efforts to investigate financial institution fraud. In 2001 the FBI investigated more than 1,300 cases in which the loss suffered by the financial institution was less than $25,000, while today we have just one case in this category. In contrast, in the past three years the number of mortgage fraud cases has climbed steadily from 1,200 in 2007 to over 3,000 in 2010, with 69 percent of the pending cases representing losses exceeding $1 million, often by a large margin. The FBI's efforts to address complex securities and corporate frauds have also greatly expanded since 2001, growing by over 1,000 cases (corporate fraud cases are up by 111% while high-yield securities fraud cases have grown by over 200%). This has been possible because of a continuing commitment to ensuring adequate staffing in the White Collar Crime (WCC) program, in which over 93% of the Agent resources are dedicated to the WCC's top four priorities: public corruption, corporate/securities/commodities fraud, health care fraud, and financial institution fraud.

b. Does the FBI have annual data on the number of agents allocated to each fraud enforcement category? If so, please provide the number of FBI agents allocated to each enforcement category from 2003 to 2008.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.034

Response:

As indicated above, the FBI does not maintain statistics addressing the categories used by the AOUSC. We do, though, maintain statistics for our WCC subprograms. Below are the numbers of Agents working in each WCC subprogram from FY 2003 through FY 2009.

Subprogram	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
Bankruptcy Fraud	27	22	19	15	17	13	11
Financial Institution Fraud	377	340	347	331	278	309	399
Health Care Fraud	286	377	400	386	398	379	384
Insurance Fraud	33	23	19	15	15	12	8
Money Laundering	48	47	44	37	33	28	21
Other Wire/Mail Fraud Schemes	257	207	145	100	67	56	48
Securities/Commodities Fraud	250	258	258	264	254	237	286
Telemarketing Fraud	28	21	16	12	10	7	4
TOTAL	**1,306**	**1,295**	**1,248**	**1,160**	**1,072**	**1,041**	**1,161**

c. Does the FBI annually compile the number of filings in each fraud enforcement category? If so, please provide the number of filings in each enforcement category from 2003 to 2008.

Response:

The FBI maintains a record of the informations and indictments by investigative classification, program, and sub-program. As noted above, the FBI does not maintain statistics addressing the categories used by the AOUSC. We do, though, maintain the requested statistics for our WCC subprograms. Below are the total numbers of informations and indictments for each WCC subprogram from FY 2003 through FY 2009.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.035

Subprogram	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
Bankruptcy Fraud	124	115	132	89	91	68	81
Financial Institution Fraud	2,091	1,941	1,713	1,514	1,300	1,301	1,578
Health Care Fraud	555	756	664	659	847	851	987
Insurance Fraud	111	100	72	56	39	73	43
Money Laundering	105	127	126	163	140	114	63
Other Wire/Mail Fraud Schemes	994	820	535	509	277	282	243
Securities/Commodities Fraud	508	585	507	497	592	519	578
Telemarketing Fraud	94	66	28	15	13	50	9
TOTAL	**4,582**	**4,510**	**3,777**	**3,502**	**3,299**	**3,258**	**3,582**

d. Are there instances where the FBI submits a fraud case to the U.S. Attorney's Office for prosecution, but the U.S. Attorney's Office declines to prosecute that particular case?

I) If so, does the FBI or the Department of Justice keep a record of the numbers and types of cases the U.S. Attorney's Office declines to prosecute?

ii) If so, are these cases categorized in the Traditional FBI Enforcement Area case types (*i.e.*, Bank Larceny, Financial Institution Embezzlement, SEC-Related Fraud)?

iii) If so, please provide the annual number of case submissions by the F.B.I. for each case type from 2003 to 2008.

Response to subparts I through iii:

Whenever possible, the FBI seeks a preliminary prosecutive opinion from the USAO early in the investigation. This allows the FBI to determine if the case has prosecutive merit without devoting resources to an investigation that will not

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.036

result in prosecution. In addition, throughout the course of all investigations, the FBI works closely with the USAO to ensure the case continues to merit prosecution.

DOJ's Executive Office for United States Attorneys (EOUSA) maintains records of the numbers and types of cases referred by the FBI for prosecution but declined by USAOs for a variety of reasons. These reasons include insufficient evidence of criminal intent, a request from the referring agency, and failure to satisfy the prosecutorial guidelines articulated in the United States Attorneys' Manual's Principles of Federal Prosecution.

Below are the numbers of USAO declinations reflected in EOUSA records from FY 2003 through FY 2009. EOUSA does not maintain statistics addressing the categories used by either the AOUSC or the FBI.

Subprogram*	**FY 2003**	**FY 2004**	**FY 2005**	**FY 2006**	**FY 2007**	**FY 2008**	**FY 2009**
Bankruptcy Fraud	291	178	200	139	138	142	151
Bank Fraud and Embezzlement	2124	1701	1768	734	560	486	388
Health Care Fraud	335	284	242	233	248	212	202
Insurance Fraud	67	48	33	36	30	19	28
Money Laundering Other	278	103	141	103	126	94	82
Securities/Commodities Fraud	129	125	91	100	114	130	85
Mortgage Fraud	**	**	**	**	**	2	103
Telemarketing Fraud	16	12	7	7	5	6	2
TOTAL	**3240**	**2451**	**2482**	**1352**	**1221**	**1091**	**1041**

* This caseload information is extracted from the United States Attorneys' Case Management System.
** The program category code for Mortgage Fraud was added to the United States Attorneys' Case Management system in July 2008. Before that time, Mortgage Fraud cases were recorded under other program category codes.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.037

Questions Posed by Senator Grassley

FBI Sentinel

The FBI continues to struggle with the development of its new case management computer system, known as Sentinel. In March, I wrote to you after learning the FBI issued a stop work order to the prime contractor on Sentinel, Lockheed Martin. The reply I received indicated this was temporary and would help ensure delivery of phase 2 by this summer.

I wrote to you again about a new stop work order just a few weeks ago. I have yet to receive a response. I have repeatedly asked for a cost estimate and a new development timetable, but continue to wait for a satisfactory response. Accordingly, I ask you to provide complete responses to the following questions regarding the development of Sentinel.

45. Provide a full cost analysis of how much taxpayer money will be necessary to complete Sentinel as original[ly] designed.

Response:

The FBI is still examining options for completing the project. Until the completion approach for Sentinel is determined, the FBI is unable to perform a cost analysis.

46. Provide an estimated timetable of how much longer it will take the FBI to finish the development of Sentinel as originally planned.

Response:

The estimated timetable is between 14 and 30 months, depending on the approach the FBI decides to use.

47. In your response to questions at the hearing, you stated, "we have to look at both the budget and the time frame down the road and determine how much of that work can or should be done by the contractors, how much of that work can and should be done by ourselves, given the new technology." How many FTEs does the FBI have working on development of Sentinel?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.038

Twenty full-time employees are currently working in the Sentinel Program Management Office on program oversight. Some of these employees have expertise that could be directly applied to the delivery of capabilities in some of the options going forward.

48. Do you believe the FBI possesses the technological know-how to develop a software system in-house? Please describe what "new technology" the FBI has that will assist in developing a case management software system in-house.

Response:

We believe the FBI possesses the required expertise. The FBI has successfully developed and deployed software systems for reporting SARs and for the management of sources. The Department of Defense recently decided to adopt Guardian, the SARs reporting system.

49. Despite your assurance at the hearing that the FBI has "endeavored both for you in this Committee and other committees to keep you apprised of everything that happens in the course of our developing this software package," the FBI has held only one Judiciary Committee staff briefing on the development of Sentinel in the couple of years. That meeting was a joint meeting with members of the Appropriations Subcommittee that oversees the FBI. Will you commit to providing more frequent updates to Committee staff regarding the development of Sentinel?

Response:

The FBI has not declined any briefing requests regarding the status of Sentinel. The FBI is committed to transparency and we have provided frequent updates to DOJ, OMB, and the staffs of our various oversight committees.

50. At the hearing, I asked you if you believed the cost of developing Sentinel would exceed $1 billion. You replied, "Certainly it would not exceed $1 billion, but I can tell you, as you pointed out, there was an overarching budget for this project." As you have repeatedly failed to provide a response to how much the projected budget for Sentinel will increase, I would like some clarification on your response. The $1 billion cap that you have now gone on record as supporting, does that include the money already spent on Sentinel and Virtual Case file, or is it limited to additional funding to complete phases 2, 3, and 4 of Sentinel?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.039

The FBI is confident that its efforts to develop a case management system, including Virtual Case File, the Sentinel costs to date, and the costs of completing the Sentinel project, will not reach $1 billion.

As the FBI has worked to develop a case management system over the past several years, technological advances have been made that the FBI hopes to leverage, taking full advantage of industry product investments and efficiencies that were not available six years ago when the Sentinel requirements were established. Over this period of time, the FBI has learned a great deal about our legacy systems and our business processes. We believe these "lessons learned" will allow the FBI to successfully develop a case management system that uses industry products developed fairly recently and specifically designed for such undertakings.

As noted above, the FBI continues to explore options that will allow us to complete the Sentinel project within or near a cost of $451 million.

51. You repeatedly spoke of "ongoing negotiations" with Lockheed Martin. When do you expect these negotiations to end?

Response:

The FBI's negotiations are primarily focused on the technical aspects of the Sentinel program. The FBI must ensure that the next steps will result in the successful development and deployment of a case management system that will serve the FBI and our national security interests for many years to come.

52. I asked you about the $25 million of taxpayer money that has been spent on the now indefinitely suspended phase 3 of Sentinel. You responded that the money "will go into our evaluation of where we go with phases 3 and 4." I think the American taxpayers deserve an answer whether the FBI will be able to recoup that money spent, especially if the FBI were to go with another contractor as you seemed to imply at the hearing. Will the FBI actively seek to recoup any money spent on phases 3 or 4 if Lockheed Martin is removed as the primary contractor? If not, why not?

Response:

The payments made to Lockheed Martin during Phase 3 funded authorized work that has been delivered to the FBI. Consequently, the FBI will not seek to recover these funds. No payments have been made, or work begun, on Phase 4.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00087 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.040

53. What role do you see Lockheed Martin playing in the development of the remaining phases of Sentinel?

Response:

Multiple approaches are being considered for Sentinel's completion. Lockheed Martin's future role will depend on the option selected.

54. At the hearing, you stated that contract modifications on the Sentinel project "are relatively minor modifications, and not the principal contributor to whatever delays there have been." Have you reviewed all the contract modifications? Do you believe there were any unnecessary contract modifications that may have resulted in delays? Do you have a plan to limit contract modifications or change orders within those modifications on phases 3 and 4? If so, please describe those plans in detail.

Response:

All contract modifications have been reviewed through multiple internal control mechanisms. The FBI does not believe there were any unnecessary contract modifications. The plan for moving forward will include control systems for change orders to ensure any requested changes are in the best interests of the government and the taxpayer. Once Sentinel's path forward has been decided, we will be able to provide greater detail regarding our plan for managing change orders.

GAO Access Problems

GAO has been attempting to conduct a review of human capital management challenges in the FBI's counterterrorism division. Specifically, Congress heard testimony that there were high vacancy rates in the division, so the House and Senate Judiciary Committees asked GAO to find out if that was true and, if so, make recommendations as to how the FBI should deal with the problem. Unfortunately, the Justice Department has blocked GAO's access to the information it needs to do this important work as Congress requested.

In answers to questions for the record you provided earlier this year, you said, "aspects of the review ... constituted intelligence oversight." You also said, "It is the longstanding position of the intelligence community to decline to participate in GAO reviews that evaluate intelligence activities."

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.041

However, other portions of the intelligence community have cooperated with GAO reviews of this sort that do not involve sources and methods. For example, GAO was able to obtain the information it needed to conduct a review that I requested of the Treasury's Office of Terrorism and Financial Intelligence.

55. I see no reason that the FBI should be exempt from GAO oversight. Do you think it should be, and if so, why?

56. I understand it is the Justice Department's Office of Legal Counsel (OLC) that has been the primary obstacle to GAO receiving the information it needs. If OLC cleared it, would you have any objection to complying the GAO's information requests?

57. GAO has attempted to resolve this issue with the Justice Department on several occasions and has even had difficulty simply scheduling meetings with the relevant officials. Would you be willing personally [to] spend some time with GAO and the Justice Department to resolve these issues and ensure that GAO gets what it needs to answer our questions?

Response to Questions 55 through 57:

The FBI endeavors to cooperate fully with GAO requests by providing any information that can be released, and we will continue to do so.

FBI Supplemental Funding Request for Agents on the Southwest Border

The U.S. Department of Justice recently submitted to Congress a FY 2010 Southwest Border Supplemental Funding Request. In your written statement, you indicated "the FBI currently has approximately 145 agents assigned to twelve border corruption task forces along the Southwest border." However, the supplemental budget request submitted by the Department asks for an additional 44 agents to be assigned to "hybrid squads" composed of gang, violent crime, and public corruption investigators. The supplemental also requests funding for tactical equipment to be used by FBI SWAT teams.

58. Will the additional 44 agents requested in the FY 2010 Department of Justice supplemental request augment the existing 145 agents assigned to the border corruption task forces you mentioned in your opening statement or will they replace retired or reassigned agents?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.042

The 44 Agents requested in the FY 2010 SWB supplemental will support hybrid squads along the SWB. These 44 Agents are in addition to the 145 Agents currently assigned to the border corruption task forces.

59. If the 44 new agents requested in the FY 2010 supplemental request are in addition to overall FBI special agent positions, does the FY 2011 budget for the FBI reflect these potential new hires?

Response:

Although the FY 2011 budget request does not reflect the funding required for these additional positions, the FBI recognizes the importance of maintaining the staffing for these hybrid squads on an ongoing basis.

60. Has the FBI assigned any agents to the Southwest border region on a temporary duty status (TDY) and if so, what are the current cost estimates for those TDY assignments?

Response:

The FBI will place three Agents and one Intelligence Analyst in 90 to 180-day temporary duty assignments in the following locations: United States Consulate, Ciudad Juarez, Chihuahua, Mexico; United States Embassy, Ciudad Mexico, Mexico; and United States Consulate, Guadalajara, Jalisco, Mexico. These assignments will provide the opportunity for FBI personnel to interact with Mexican authorities on a daily basis in order to obtain valuable intelligence regarding violent crime matters. The estimated cost of these temporary assignments is approximately $4,200 a month per FBI employee assigned to the Ciudad Juarez/El Paso, Texas, area and approximately $8,000 a month per FBI employee assigned to Ciudad Mexico and Guadalajara.

Also, since mid-March 2010, approximately 29 FBI employees have been assigned to assist in the Ciudad Juarez Consulate murder investigation. The average cost for each of these employees is approximately $5,000 per month.

61. Does assigning 44 new agents to the Southwest border subtract from the FBI's mission to combat and detect counterterrorism both domestically and abroad?

Response:

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.043

The FBI's top priority is protecting the U.S. from terrorist attack, and all decisions regarding resource allocation are made consistent with that priority.

62. How many of the FBI agents assigned to the Southwest border region are currently assigned to the FBI SWAT team and of the requested 44 new agents, how many of those will be assigned to the FBI SWAT team?

Response:

Currently 188 FBI SWAT operators are assigned to the eight FBI SWB field offices. Each of the FBI's 56 field divisions has a SWAT team, with SWAT duties being ancillary to an Agent's investigative responsibilities. All interested Agents may compete for SWAT team vacancies in their divisions. If any of the Agents assigned to the newly formed squads in the SWB region are already SWAT operators, these Agents will continue to serve in that capacity.

63. Will the 44 new FBI agents assigned to the Southwest border region be assigned hazardous duty pay if they are required to work extensively in Mexico? If so, is that also reflected in the FY 2011 FBI budget request?

Response:

The FBI Agents assigned to the SWB region will be entitled to receive Danger Pay if they are assigned to work in Mexico. However, because the SWB Supplemental positions are domestic positions, additional Danger Pay for long-term foreign assignments is not included in the FY 2010/2011 SWB Supplemental Appropriation. Due to the nature of the domestic cost module, the FBI does not intend to request Danger Pay through the standard personnel annualization of positions in the future. Instead, any additional Danger Pay required to support these positions will be funded through FBI's base funding.

Questions Posed by Senator Kyl

64. The media has recently reported that the administration may seek to add "electronic communications transactional records" to the list of information that the FBI may request pursuant to 18 U.S.C. § 2709(b)(1).

a. Please explain why the administration believes that this language should be added to the statute.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.044

Response:

The Administration wishes to amend 18 U.S.C. § 2709(b)(1) to ensure consistency between the types of records National Security Letter (NSL) recipients are required to provide to the FBI under 18 U.S.C. § 2709(a) and the types of records that are subject to the procedural protection of an FBI certification of relevance pursuant to 18 U.S.C. § 2709(b)(1).

Congress enacted Section 2709 in 1986 to allow the Government to obtain telephone toll and transactional records in national security investigations upon proper certification by the FBI Director or his designee. As originally enacted, subsection (a) established a requirement for wire and electronic communication service providers to comply with an FBI request for "subscriber information and toll billing records information, or electronic communications transactional records." Subsection (b), which provided the means by which the FBI could make such requests, did not specify what information the FBI must certify is relevant. Instead, it required certification that "any such information and records," as described in subsection (a), were relevant to an investigation. When Congress amended subsection (b)(1) in 1993, among other things, it replaced the term "any such information and records" with "name, address, length of service, and local and long distance toll billing records," failing to include the term "electronic communications transactional records." While subsection (a) still required production of electronic communications transactional records, the omission of the phrase "or electronic communications transactional records" left subsection (b) without any reference to such records.

b. What kinds of "electronic communications transactional records" does the FBI want to obtain?

Response:

The FBI does not seek to obtain the contents of electronic communications. We do, though, want to continue to obtain electronic communications transactional records (ECTRs) that will facilitate our national security investigations - records that we have received routinely for years. We are, therefore, seeking a change in section 2709(b)(1) to clarify the authority we already have to obtain ECTRs.

A change to section 2709 is necessary to clarify the obligation of electronic communications service providers (ECSP) to provide ECTRs pursuant to 18 U.S.C. § 2709(a). Currently, 18 U.S.C. § 2709(a) does not work synchronously

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.045

with section 2709(b)(1). The lack of synchrony between subsections (a) and (b)(1) has led ECSPs to conclude that the FBI is not entitled to obtain ECTRs but may only obtain the "name, address, and length of service." In comparison, it has led one court to the other extreme, suggesting in dicta that ECSPs might have an obligation to provide the FBI with ECTRs *even absent* FBI compliance with the procedural protections in subsection (b)(1). (See Doe v. Gonzalez, 500 F. Supp. 2d 379, 387 (S.D.N.Y. 2007).) The FBI believes neither extreme is correct. It appears Congress intended that the FBI be able to use an NSL to get ECTRs (that are parallel to telephone toll billing records, including "to" and "from" records or records that an ECSP could use to bill a particular account) and that the certification and other procedural protections contained in subsection (b) would apply. Without the proposed amendment, however, the statute creates uncertainties that hinder the FBI's ability to conduct effective national security investigations.

c. Please describe the national security risks, if any, that would result from the FBI's inability to obtain "electronic communications transactional records" under 18 U.S.C. § 2709(b)(1).

Response:

The FBI's ability to conduct national security investigations will be significantly impaired if it is unable to obtain promptly all ECTRs currently obtainable under section 2709. NSLs are thought of as "building blocks" of national security investigations because they are generally used early in such investigations to develop leads and to determine a subject's associates and financial dealings. This information is critical to understanding whether and to what extent the subject of a national security investigation is involved in a threat to national security and the nature of the threat. Just as critical, the information obtained through NSLs is used to remove individuals from suspicion. Because the FBI is unable to obtain certain ECTRs with an NSL, it takes investigators longer to determine what connection, if any, a subject has to a potential national security threat, including a threat of terrorist attack. The FBI does not always know at the beginning of an investigation whether the target poses an immediate or long-term threat. For that reason, one of the tools the FBI needs to conduct effective national security investigations is the ability to obtain ECTRs through the use of NSLs.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.046

SUBMISSIONS FOR THE RECORD

STATEMENT OF SENATOR PATRICK LEAHY (D-VT.),
CHAIRMAN, SENATE JUDICIARY COMMITTEE
HEARING ON OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION
JULY 28, 2010

Today the Judiciary Committee hears from Director Robert Mueller of the Federal Bureau of Investigation (FBI) for the fourth time this Congress. We held two FBI oversight hearings last year, and the Director appeared earlier this year to testify about national security issues. We welcome Director Mueller back to the Committee.

Oversight is one of Congress's most important responsibilities, and one that this Committee continues to take seriously. Along with regular appearances from Director Mueller, the Committee has held multiple oversight hearings with Attorney General Holder, oversight hearings with Homeland Security Secretary Napolitano, the heads of key components of the Justice Department, and other senior executive branch officials.

I appreciate Director Mueller's continued openness to oversight and accountability as we work together to ensure that the FBI is able to effectively pursue its critical missions in law enforcement and national security, while maintaining the freedoms and values that define us as Americans. Director Mueller has worked to close the longstanding gaps in responses to written questions, inquiries, and document requests from this Committee. More work remains to be done, but the increased openness and responsiveness from the FBI helps both the Bureau and Congress to do their jobs more effectively.

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 in recent months a series of important arrests of those who would do this country harm.

Just last week, the FBI announced the arrest of Zachary Chesser, an American who sought to join a terrorist organization in Somalia. The FBI had been monitoring Chesser for months. It appears from court documents and public statements that in this case, the system worked as it should. Mr. Chesser was watched carefully through court approved surveillance, was placed on the "no fly" list, and was arrested as he tried to fly to Africa. Cases like these reinforce my conviction that criminal investigations and prosecutions are vital weapons in our national security arsenal.

In this Congress, we have made great strides toward more effective fraud prevention and enforcement. I worked hard with Senators Grassley, Kaufman, and others to craft and pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade, which the President signed into law last spring. That important legislation added resources and statutory tools for effective prevention, detection, and enforcement of mortgage fraud and financial fraud. The same bipartisan group of Senators worked hard this year to ensure that the landmark healthcare reform legislation included important new tools for cracking down on health care fraud, and that the historic Wall Street reform legislation the President just signed included key measures to strengthen enforcement of securities fraud and bank fraud.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.047

I am pleased to see that the FBI has been taking full advantage of this heightened support for and focus on fraud enforcement. This spring, the Attorney General told Congress that, in part as a result of the recently passed legislation, the FBI has more than doubled the number of agents investigating fraud. Since 2007, the Justice Department's health care fraud strike forces have sent more than 205 defendants to prison and have significantly deterred Medicare fraud. Earlier this month, the Department charged 94 defendants with cheating the Medicare system of more than $251 million dollars in the largest health care fraud sting ever.

I congratulate the Director for the FBI's central role in these successful investigations, and 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 that has devastated so many hard-working Americans.

Combating corruption has long been another important priority for the FBI. I was very disappointed that the Supreme Court last month undermined these efforts by siding with Enron executive Jeffrey Skilling, and greatly limiting a statute vital to federal efforts to crack down on corruption and fraud. I hope Director Mueller will work with me and with members of this Committee to fix the gaps that the Supreme Court has left in the law.

I have also 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 since the infusion of federal support in last year's recovery legislation and in the appropriations process has been vital to keeping crime down throughout the country.

Areas of major concern remain, however. The FBI continues to struggle with efforts to modernize its technology and information-sharing systems, wasting valuable time and precious taxpayer money. The Sentinel program appears to be the latest in a series of FBI technology initiatives to fail. I was distressed to learn that the FBI has felt it necessary to suspend work orders and essentially start over yet again. While it is a good sign that the Bureau is taking affirmative steps to take control of the situation, it is alarming that we have again gotten to this point. I hope the Director can assure us there is a plan to get this disastrous project on track once and for all.

I also was distressed to hear press reports this morning about widespread allegations of cheating on a test that is meant to ensure that FBI agents understand the limits on their investigative authorities. I hope the Director can shed some light today on these alarming reports.

I thank Director Mueller for returning to the Committee, for his responsiveness to our oversight efforts, and for his personal example and leadership 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 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.048

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

July 28, 2010

The Honorable Richard J. Durbin
United States Senate
Washington, D.C. 20510

Dear Senator Durbin:

Upon reviewing the transcript of the hearing today, Director Mueller realized that he misspoke. You asked the Director whether there is a requirement of "suspicion of wrongdoing" in order for the FBI to engage in surveillance of an individual or location under the FBI's Domestic Investigation and Operations Guide (DIOG). His answer should have been that there must be a proper purpose for the surveillance. Suspicion of wrongdoing could be a proper purpose, but it is not the only proper purpose. Further, as noted in the Director's answer to the next question, membership in a certain religion or ethnic group is not, standing alone, a proper purpose.

This correction will be made a part of the official transcript of the hearing.

Sincerely,

Stephen Kelly
Assistant Director
Office of Congressional Affairs

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

1 - The Honorable Jeff Sessions
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 23, 2010

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 before the Committee on March 5, 2008. We apologize for the lengthy delay and hope that this information is of assistance to the Committee.

Please note that these responses are current as of June 27, 2008, and more recent information may be available in Director Mueller's testimony before the Committee on September 16, 2009 and January 20, 2010. Copies of the Director's statements for the record from those more recent hearings are enclosed. Please also note that these responses exclude the responses that were provided to the Committee on September 16, 2008.

Please do not hesitate to call upon us if we may be of additional assistance. Since these responses are current only through June 27, 2008, they have not been cleared by the Administration. The Office of Management and Budget has no objection to our submitting these responses to the Committee with that caveat.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Jeff Sessions
Ranking Minority Member

Responses of the Federal Bureau of Investigation to Questions for the Record From the March 5, 2008 Hearing Before the Senate Committee on the Judiciary Regarding Oversight of the FBI

Questions Posed by Chairman Leahy

Biometric Database

1. The FBI announced last month that it had awarded a $1 billion contract to Lockheed Martin to develop the Next Generation Identification database, a massive database of biometric information – starting with fingerprints, but expanding to include palm prints and perhaps facial features, retinal scans, and other forms of identification. This is a program that was never directly authorized by Congress and that is therefore subject to few checks or reporting requirements. Do you agree that appropriate oversight and legislation if necessary concerning this program, including regular reporting requirements, progress reports, audits, and privacy safeguards, would help the FBI to more effectively implement this database and to avoid the problems we have seen in other ambitious but unregulated initiatives?

Response:

Congress discussed the FBI's development of the Next Generation Integrated Automated Fingerprint Identification System (IAFIS), now referred to as Next Generation Identification (NGI), in the Fiscal Year (FY) 2005, 2006, 2007, and 2008 Appropriations Acts. For example, the Conference Report associated with the FY 2006 Appropriations Act (Public Law 109-108) stated:

> The conferees support the FBI's efforts to improve the speed and accuracy of IAFIS, expand the data available in the system, and improve its latent print capabilities. The conferees direct the FBI to use excess user fee collections from various Criminal Justice Information Services' programs to fully fund the Next Generation IAFIS project in fiscal year

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.051

2006 including the $16,808,000 requested program increase.

The FBI has provided information to Congress regarding the NGI program through briefings and other means on several occasions, has participated in both internal and external audits, and has multiple quality and cost control mechanisms in place. We would be pleased to provide additional briefings upon request.

2. The FBI collects fingerprints of many government employees and others who go through security clearances. The Defense Department collects fingerprints of military personnel. Presumably in the future, the government will collect other biometric identifying information of the men and women who serve our country. Right now, that information does not go into the FBI's database, but that could easily change. What assurances can you give that identifying information of government employees and military personnel will not go into this new database?

Response:

The FBI has collected the fingerprints of Federal government employees, including those of military personnel, for decades. In 1941, Executive Order (EO) 8781 (6/12/41) required that all executive civil service applicants and employees be fingerprinted and that these fingerprints be transmitted to the FBI for criminal record checks and for permanent retention (later EOs authorized exemptions for temporary employees). Pursuant to EO 10450 (4/27/53), Federal employees are subject to investigation to protect national security including, at a minimum, a national agency check (including a check of the FBI's fingerprint files). 28 U.S.C. § 534(a)(1) requires the Attorney General (AG) to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records."

NGI will support the collection of additional biometric data, to potentially include data collected for Federal employment and military service, as permitted by the authorities currently in place. Although fingerprint data will remain the primary means of identification, the collection of additional biometric data will be used for investigative purposes and to assist in the identification process. The FBI will retain additional biometric data when the authorized submitting agency submits such data for retention purposes.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.052

3. Currently, fingerprints are generally collected in the criminal justice system when people are arrested, and those fingerprints go into the FBI's database. Of course, when someone is arrested, often no charges are brought, or the person is found innocent. Yet many innocent people who have the misfortune of being arrested at some point may now be deprived of their civil liberties and right to privacy. Their most sensitive personal identifying information will apparently be kept in a government database unless they go through a cumbersome procedure to try to get themselves removed from it.

a. Why does the FBI keep information in its database about people who are arrested but never convicted?

Response:

As noted in the response to Question 2, 28 U.S.C. § 534(a)(1) requires the AG to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." As a general rule, the FBI maintains fingerprints in order to perform identification and criminal history record information functions, including background investigations and suitability determinations conducted pursuant to Federal and state law, and the provision of humanitarian identification assistance, such as occurs following a natural or man-made disaster. With regard to fingerprints and other information about persons who are arrested but not convicted, in particular, an "arrest" is a matter of record and is retained as such by police agencies throughout the country. It is fundamental to effective police work and to the administration of criminal justice when investigating, arresting, or prosecuting an individual to determine whether he or she has been arrested before for the same or similar crimes. In addition, the arrest record and its details may become critical evidence for a party on either side of a civil suit. For these reasons, through the statute cited above, Congress directed the AG to preserve these records and make them accessible nationally. The preservation of fingerprints is discussed in the Privacy Act notice for the FBI's fingerprint database (Justice/FBI-009, 64 Fed. Reg. 52347 (9/28/99)), which includes a description of the ways fingerprints can be used and references the means by which an individual can correct or update a fingerprint record (see 28 C.F.R. § 16.34), providing transparency regarding the ways in which the FBI uses fingerprints. Court challenges to the FBI's maintenance of fingerprints have generally been unsuccessful, with the courts consistently finding that, absent an expungement order, there is no basis for returning or destroying arrest, fingerprint, or related records. Expungement is a remedy afforded by the courts

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.053

based upon a case-by-case balancing of an individual's need for privacy against the government's need for the records for effective law enforcement.

Wiretaps/Telephone Bills

4. In a January report, Department of Justice Inspector General Glenn Fine found many instances when the FBI failed to pay its telephone bills in foreign intelligence and undercover cases, sometimes resulting in wiretaps being cut off. He found that in more than half of nearly 1,000 confidential case files reviewed, bills were paid late. In a number of cases, electronic surveillance was cut off because of late payments, including at least one instance of a wiretap under FISA. What steps are being taken to ensure that all telephone bills are paid on time, and no criminal or national security wiretaps are cut off in the future?

Response:

The report by the Department of Justice (DOJ) Office of the Inspector General (OIG) presents an opportunity for the FBI to accelerate improvements in the internal controls related to our telecommunication payments that are already underway and to aggressively pursue additional means of improving this process. Surveillance interruptions due to nonpayment are rare, and the risk of losing evidence because of an interruption due to nonpayment is even more remote. This risk has been further reduced by improvements to the processes and internal controls initiated both before and in the wake of the OIG's recommendations.

In July 2006, DOJ's OIG initiated an audit of the FBI focused on undercover activities funded by field office confidential funds from 2004 through 2006. This audit resulted in 16 recommendations to improve the FBI's internal financial controls related to case funds and to the tracking, processing, and paying of undercover telecommunications expenses. All 16 recommendations have been closed or resolved and the FBI has taken steps, many of which are independent of the OIG audit, to improve processes and provide additional oversight of confidential case fund use.

Efforts to address the OIG's concerns include the following.

- Establishing standard operating procedures for paying telecommunications costs.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.054

- Mandating the use of the Technical Management Database to bring consistency and transparency to the management of technical programs by FBI field offices.

- Conducting internal audits, through the FBI's Inspection Division, of the use of the Technical Management Database and the payment of covert telecommunications bills.

- Enhancing field office financial training.

Bullet Lead Analysis

6. Will you commit that the FBI will comprehensively review all its past and present forensic practices and act quickly and decisively to identify and correct any possible injustice resulting from faulty forensic practices?

Response:

Please see the response to Question 5. The FBI's Laboratory is thoroughly committed to ensuring the reliability and viability of all of its forensic practices and individual case results. The FBI's Laboratory is accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board, which requires that each accredited laboratory have at its core a vigorous quality control system that uses validated procedures and continuous audits. Under this system, examiners and technicians are subject to routine proficiency testing; every laboratory report must undergo thorough technical and administrative review before it is approved for release to the contributor; and each forensic discipline must maintain and constantly review standard operating procedures, which must be followed and documented in every exam. In addition, ongoing review groups continue to thoroughly review the "experience-based" disciplines, and a new testimony monitoring system strives to ensure that examiners are consistently providing thorough and accurate court testimony.

National Security Letters/Exigent Letters

7. Last year, the Department of Justice Inspector General found improper use of National Security Letters by the FBI in more than one in five of the files reviewed. A more detailed

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.055

FBI internal audit reached nearly the same conclusion. It is now clear that there have been thousands of instances where the FBI did not follow its own rules in issuing NSLs and hundreds, if not thousands, of cases where these violations should have been reported to the President's Intelligence Oversight Board.

a. Do you agree that there needs to be some independent oversight of the National Security Letter process -- oversight from outside the FBI -- to make sure the FBI follows the law and its own internal policies in issuing National Security Letters?

Response:

Before addressing the issue of oversight, it is important to put the incidents/errors detected during the course of the various reviews in context. While the FBI took very seriously the findings in the Inspector General's (IG) 2007 report, it is not accurate to say the IG found thousands of instances in which the FBI did not "follow its own rules" in issuing National Security Letters (NSLs). Putting aside the use of so-called "exigent letters," which was a significant problem that involved primarily one FBI Headquarters unit and is being investigated by the IG, the majority of the problems identified by both the IG and the FBI's internal reviews involved either: a) FBI errors that did not affect whether the FBI was entitled to obtain the requested information, or b) the overproduction of information by third-party recipients.

For the 2007 report, the OIG sampled 293 NSLs and identified 22 potential violations. Of those 22 potential violations, 10 were third-party overproductions, leaving a net potential FBI violation rate of 4%. While a 4% error rate is unacceptable, it is important to note that only 5 of the errors (1.7% of the total sample) involved errors that resulted in the FBI obtaining information it was not authorized to obtain. The balance involved errors that reflected a lack of attention to detail. While the overall error rate is low, we believe the addition to the FISA Management System of the new NSL subsystem will reduce this rate even further. Use of this subsystem was mandated in 2008, and it should reduce or eliminate many of the common errors found in the course of the OIG and internal FBI audits. The subsystem provides a web-based entry page in which all information required for Congressional reporting must be entered. In order for the NSL to be issued, all officials required to approve an NSL by statute or FBI policy must approve the NSL within the subsystem. If the required information is not entered, or if required approvals have not been registered, the subsystem will not generate

an NSL. The subsystem will also reject common errors, such as citing a counterintelligence investigation when the drafter is seeking a credit report using a Fair Credit Reporting Act NSL, or citing a control file rather than an investigative file. In addition, because the NSL and the NSL approval memorandum are created from the same data set, the use of this subsystem will reduce typographical errors and incorrect or inconsistent statutory citations. The IG's 2007 findings were largely confirmed through the FBI's own internal audit. Looking at a far larger sample (10% of all NSLs issued from 2003 through 2006), the FBI detected an overall error rate of approximately 10% (759/7863). Significantly, however, the vast majority of these 759 errors involved third-party overproduction (676/759). When the third-party overproduction is removed, the internal audit detected 83 "FBI errors," which is an error rate of 1.05% – slightly lower than the error rate detected by the IG in his much smaller sample.

Although the most recent OIG report, issued in March 2008, disagreed somewhat with the findings of the FBI's internal review, the fact remains that the rate of substantive error by the FBI in issuing NSLs (defined as errors that result in the FBI obtaining information to which it is not legally entitled) does not lead to the conclusion that the imposition of external controls on the use of NSLs is necessary, particularly given the substantially improved internal controls the FBI has implemented in this area (discussed in detail below).

Substantial independent oversight already exists in the form of DOJ's IG and National Security Division (NSD). As indicated above, DOJ's IG has identified compliance issues and made recommendations for improvement, which have led to changes in FBI policy, training, and procedures to enhance compliance. In addition, together with attorneys from the FBI's National Security Law Branch (NSLB), DOJ's NSD is conducting regular National Security Reviews of FBI field offices and Headquarters elements. The NSD and NSLB conducted 15 of these reviews in 2007 and have scheduled an additional 15 in 2008. That rate of review is expected to continue in future years. During these reviews, attorneys from the NSD and NSLB examine the use of NSLs, FBI compliance with AG guidelines on national security, predication for national security investigations, and referrals to the Intelligence Oversight Board (IOB). Specifically regarding NSLs, the NSD and NSLB examine FBI files to determine whether NSLs were correctly and appropriately drafted and approved and whether the results provided in response to NSLs were within the scope of the requests. DOJ's Office of

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.057

Privacy and Civil Liberties participated in the 2007 reviews and will be briefed on the results of the 2008 reviews.

In addition to DOJ oversight, the FBI reports violations of the Constitution, the laws of the United States, Executive Orders, and Presidential Directives to the IOB, which is charged, among other things, with reviewing violations of law by members of the Intelligence Community. The FBI reports to the IOB on a quarterly basis, and violations of the NSL statutes by FBI personnel are included in these reports.

In addition to external oversight regarding the use of NSLs, the FBI has instituted a number of changes to internal policies and procedures to ensure compliance with the NSL statutes. The FBI now requires that every NSL be reviewed by an FBI attorney to confirm that the NSL meets legal and procedural requirements. In addition, the now-mandated NSL subsystem of the Foreign Intelligence Surveillance Act (FISA) Management System (an automated workflow tool) will not allow an NSL to be created unless certain required conditions are met, including legal review. The FBI has engaged in an extensive effort to train employees on the law and procedures governing the use of NSLs, including the development of a web-based training course employees must take when they begin jobs involving the issuance of NSLs. The FBI has also created an Office of Integrity and Compliance responsible for identifying high-risk areas and for changing policies, procedures, and training (if appropriate) in order to mitigate risk. In addition, the FBI's Inspection Division is adding NSL compliance to its periodic inspections.

b. Based on the Inspector General's report and your only internal audit, how many violations of FBI policy have you found with regard to National Security Letters, and how many of them have now been reported to the President's Intelligence Oversight Board?

Response:

The FBI does not maintain a separate tally of the number of NSL errors that involve violations of internal policies. In contrast with statutory or constitutional violations, violations of internal FBI policy do not require a report to the IOB.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.058

Considering specifically the 22 potential violations reported by the OIG in 2007, 5 were substantive errors that violated both the law and FBI policy and were reported to the IOB, 10 were third-party overproduction errors, and 7 involved a variety of errors that could all be considered to be violations of FBI policy. In the FBI's internal NSL review, 83 FBI errors were discovered (as opposed to third-party overproduction errors), of which 64 were substantive errors that violated the law and are reportable to the IOB. The other 19 appear to have involved typographical errors that resulted in the FBI obtaining information to which it was not entitled (that is, the typographical error resulted in requests for information not relevant to an authorized investigation). If determined to have been accurately reported during the audit, these 19 instances will be reportable to the IOB. The adjudication process is still ongoing.

c. In your internal review of this problem, have you found additional types of violation not identified by the Inspector General? If so, what have you done to report them to Congress and to correct them?

Response:

The FBI's internal review found the same types of errors as those identified by the IG. NSL errors that involve violations of law or Executive Order are reportable to the IOB, and the vast majority of potential IOB reports involve third-party overproduction or the issuance of an NSL after the relevant investigation has "lapsed." (As used here, a "lapsed" investigation is an investigation that, while properly predicated, continued beyond the period provided in the AG Guidelines without an approved and timely extension.)

The corrective actions taken by the FBI relative to NSL errors are discussed at length in response to Question 7a, above.

8. The Inspector General will issue follow up reports on National Security Letters in the coming months, including a report which will focus, in part, on the so-called "exigent letters" that were the among the most serious abuses uncovered in the initial report. The FBI sent these "exigent" letters, which are not authorized in any statute, in at least 739 instances to telephone companies in place of National Security Letters or grand jury subpoenas. In each case, the letters falsely stated that a subpoena would be issued for records, which never happened, or that a significant emergency existed, which in many cases was not true. I understand that the FBI has now banned the use of "exigent" letters.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.059

a. Do you agree with me that these exigent letters contained false information and resulted in the FBI improperly obtaining a large volume of information?

Response:

A significant number of the exigent letters issued by the FBI were either followed by, or issued contemporaneously with, grand jury subpoenas or NSLs requesting toll billing information on the same phone numbers. In addition, many of the exigent letters were, in fact, issued under conditions that would meet the emergency disclosure standard of section 2702(c)(4) of the Electronic Communications Privacy Act. This provision allows an electronic service provider to provide records voluntarily to the government in emergency situations.

Nevertheless, many of the exigent letters included inaccurate information. In many cases, no grand jury subpoena or NSL was subsequently issued, and in many cases no emergency existed with regard to the number about which we sought toll billing information.

The FBI is currently reviewing all of the numbers that were the subjects of the exigent letters to determine whether there is any legal basis for retaining the information provided in response. For additional information regarding this process, please see the responses to Questions 8b and 8c, below.

b. What has the FBI done to make sure that the information illegally obtained by the "exigent" letters has been purged from the FBI's databases and computer systems?

Response:

The FBI is currently taking steps to address the issues raised by the use of so-called "exigent letters." The FBI is removing information it has no legal authority to retain. Purging the toll records related to a number solely because the number was the subject of an exigent letter, however, would be an overbroad reaction, as it would require the FBI to purge some information the FBI can legally retain that is or may be of value to international terrorism or counterintelligence investigations. The process the FBI is following to rectify the exigent letter

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.060

situation has been described to the DOJ IG, other appropriate parties in DOJ, and the IOB, and briefed to the House and Senate Judiciary and Intelligence Committees, and the documentation related to these record reviews either has been or will be provided to DOJ's IG.

The process includes several elements. A team of FBI analysts and attorneys is reviewing every number for which toll records are known to have been requested by such letters. For each number, the team is checking FBI databases to identify cases to which the information is relevant, to determine whether other legal process may have been used to obtain the toll record information, and to ascertain whether an emergency situation existed at the time the records were sought through the exigent letter process.

If the review determines that other legal process (a grand jury subpoena or NSL) was lawfully issued that covered the same scope of records as were obtained with an exigent letter, then the responsive records will be retained. If no other legal process can be located but the toll records at issue continue to be relevant to an open national security investigation, the FBI will issue corrective NSLs to the carriers. These NSLs do not request any additional records, but instead provide legal authority for the retention of the relevant records. (An alternative approach would have been to remove the records received through exigent letters and then issue new NSLs, obtain the same records again, and reload them into our systems. That approach was rejected as inefficient.) These corrective NSLs are accompanied by memoranda that document the relevance of the information sought to a national security investigation and provide the information necessary for Congressional reporting. If the FBI determines that the records related to "an emergency involving danger of death or serious physical injury to any person," they will be retained pursuant to section 2702(c)(4) of the Electronic Communications Privacy Act. In the event no other legal process is found, there is no open national security investigation to which the toll records are relevant, and there was no emergency linked to the information obtained, the information is removed from FBI systems.

c. What steps have been taken to determine how agents were authorized to issue these clearly improper "exigent" letters and to discipline those who authorized this practice?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.061

Response:

This matter remains under investigation by DOJ's IG, which has advised that it will evaluate the processes that led to the issuance of exigent letters, improper blanket NSLs, and other improper requests for information. The FBI will defer comment until that evaluation is complete.

White Collar Crime Enforcement/Violent Crime Enforcement

9. According to recent studies and press accounts, white collar crime enforcement has diminished since 9/11 because scarce FBI resources have been shifted away from the pursuit of time-consuming fraud and public corruption cases to counterterrorism. The *Seattle Times-Intelligencer* recently reported that the FBI has failed to replace at least 2,400 agents transferred to counterterrorism squads since 9/11, leaving far fewer agents to pursue other kinds of cases. A study by the nonpartisan research group Transactional Records Access Clearinghouse (TRAC) found that the prosecution of all kinds of white collar crimes is down 27 percent since 2000, and official corruption cases have dropped in the same period by 14 percent. Investigating and prosecuting terrorism cases must be a top law enforcement priority, but it cannot come at the expense of vigilant criminal enforcement here at home, including the critical area of making sure that our elected officials and government employees are not compromised.

a. What steps have you taken since 9/11 to ensure that the FBI continues to vigorously investigate sophisticated fraud, identity theft, embezzlement, and public corruption in light of the dramatic increase in focus on counterterrorism work by the FBI in recent years?

Response:

After the attacks of 9/11/01, the FBI established its top ten priorities to ensure that our resources were committed to the areas most critical to the protection of the American people. While protection against terrorist attack is the FBI's top priority, it is not our only priority. The top ten priorities include the areas highlighted in the question, which have been resourced in recognition of that clear importance. For example, public corruption investigations have received dramatically increased resources; in 2007, 645 FBI Agents were assigned to investigate public corruption violations; a 53% increase over 2003 resources. As a consequence, in FY 2007 public corruption programs recorded 1,084

These responses are current as of 6/22/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.062

indictments and informations, a 40% increase over 2003 numbers. This trend appears to be continuing - in mid-2008 almost 2,500 public corruption cases were pending, which is a 49% increase over 2003.

Fraud and other white collar crimes are also receiving the resources necessary to address emerging and escalating criminal activity. For example, the FBI is addressing the systemic, long-term, multibillion-dollar contract corruption and procurement fraud in the Middle East by initiating over 55 investigations related to fraud in the Global War on Terror, a substantial increase over prior years.

Decreases in some programs have occurred, but are not necessarily related to post-9/11/01 reassignments. For example, the FBI's Health Care Fraud Program had a Funded Staffing Level (FSL) of 449 Special Agents (SAs) in 2003, which has since been reduced to 400 SAs. This decrease is, though, predominantly a function of the FBI's need to work within the constraints of the Health Insurance Portability and Accountability Act of 1996, rather than of post-9/11 reassignments.

b. The FBI and U.S. Attorneys' Offices in recent years have also had to divert resources away from criminal law priorities and into counterterrorism. The diversion of resources has come at the expense of vigilant enforcement of crime right here at home. Several recent studies indicate that violent crime rates in this country are rising. Has the FBI now replaced all of the agents who have been diverted since 9/11 from criminal law enforcement towards counterterrorism? If not, why not?

Response:

Although the FBI remains committed to its criminal programs, counterterrorism is the FBI's top priority. That said, the FBI takes seriously its responsibility to work in partnership with state and local law enforcement to reduce violent crime. The FY 2007 Preliminary Uniform Crime Report reflects a 1.4% decrease in the number of violent crimes, and much of that decrease can be attributed to law enforcement efforts. Some communities continue to face violent crime challenges, however. To help the FBI respond quickly and effectively to those areas, we have asked the Science and Technology Policy Institute, a research and analysis group run by the Institute for Defense Analyses, to conduct a detailed study of violent crime trends across the nation. Although the study is on-going, initial information suggests that the apparent increase in violent crime between

2004 and 2006 may have occurred predominantly in a small group of select cities and may not constitute a nationwide trend. Additionally, if the simultaneous rate of population increase in these areas is taken into account, the degree to which violent crime has increased is further reduced.

c. In light of the diversion of resources since 9/11, what steps have you taken to ensure that the FBI continues to vigorously investigate violent crime?

Response:

While the FBI's resources have been realigned to address terrorism in the wake of the attacks of 9/11/01, the FBI has remained committed to the aggressive investigation of the most serious violent crimes. To fulfill this commitment, the FBI has emphasized a task force approach involving a significant increase in our Safe Street Task Force operations that target gangs and other violent crime threats. These task forces are comprised of Federal, state, and local investigators, acting as a force multiplier to combine and focus valuable resources on the most significant threats to our communities. The FBI currently manages and leads 143 Violent Gang Safe Streets Task Forces (VGSSTFs) (an increase of 93 since 2001), which employ a total of 1,243 state and local task force officers (TFOs). In addition, the FBI aggressively operates 41 Violent Crime Safe Street Task Forces (with 282 TFOs), 16 Safe Trails Task Forces (with 130 TFOs), 23 Child Prostitution Task Forces (with 184 TFOs), and nine Major Theft Task Forces (with 66 TFOs).

Cyber Crime

10. In your written testimony, you stated that protecting the United States from cyber-based attacks and high-technology crimes is the FBI's third top priority. Last December, the Senate unanimously passed a bipartisan anti-cyber crime bill to strengthen the tools available to government investigators and prosecutors to combat cyber crime. The *Identity Theft Enforcement and Restitution Act, S. 2168,* would, among other things, give victims of identity theft the ability to seek restitution for the loss of time and money spent restoring credit and remedying the harms of identity theft and amend sections 1028(a), 1028A, 1030(a) and 3663(b)(6) and 3663A(b)(5) of the federal criminal code to expand the jurisdiction of federal computer fraud statutes to cover business organizations. This bill is endorsed by the Department of Justice and numerous high tech, consumer and privacy

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.064

groups. Do you support the Identity Theft Enforcement and Restitution Act, and will you work to ensure that this anti-cyber crime legislation is enacted into law this year?

Response:

The FBI supports DOJ's articulated view on this legislation.

Investigations Into Private Security Contractors

12. According to press accounts, the FBI's initial inquiry into the killing of 17 unarmed Iraqi civilians at Nisoor Square in Bag[h]dad last September by employees of Blackwater, a private security contractor, concluded that at least 14 of the 17 deaths were unjustified. As publicly reported, there is an ongoing criminal grand jury investigation into the matter, and FBI agents two weeks ago returned to Bag[h]dad for more interviews of victims and other witnesses to the incident. In December, officials from the Justice Department and State Department told the House Judiciary Committee that there were legal obstacles to the prosecution of Blackwater security guards. These obstacles include a limited form of immunity given by the State Department to Blackwater suspects during the initial inquiry into the killings, as well as problems asserting jurisdiction over private security contractors who are not currently held fully accountable under U.S. law.

a. Does the FBI grant immunity like that granted here by the State Department during its initial interviews of suspects in a criminal investigation?

Response:

It is the FBI's understanding that the premise of the question is inaccurate, as the Department of State (DOS) did not grant criminal immunity in this case. That said, the FBI does not grant "immunity" during its interviews of suspects in criminal investigations. The FBI does, though, interview suspects during "proffer" sessions in which a DOJ attorney has officially advised the suspect and his or her attorney that the information he or she provides during that particular interview, or series of interviews, will not be used in subsequent Federal prosecution of the suspect. The purpose of these "proffer" interviews is to acquire information or cooperation that would be difficult or impossible to obtain otherwise.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00112 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.065

b. Do you believe the immunity granted by the State Department has hindered your investigation or will hinder a prosecution?

Response:

As indicated above, it is the FBI's understanding that the premise of the question is inaccurate, as DOS did not grant criminal immunity in this case. While we understand that certain Blackwater guards may have been provided warnings that may create evidentiary challenges, it is our understanding that DOS was not authorized to, and did not, grant immunity. That said, if immunity were granted, such a grant would be both a legal and strategic matter under the purview of government prosecutors, and the FBI would not have a position on whether the immunity grant hindered prosecution.

c. Do you believe that the limits of U.S. jurisdiction over private security contractors in Iraq will hinder the investigation and prosecution?

Response:

We cannot comment on the details of ongoing investigations, but note that, at times, jurisdiction limits adversely affect prosecution.

13. Congress is currently considering legislation to hold private security contractors more accountable, not only in Iraq, but in all regions in which the United States has decided to use them. This legislation would amend the Military Extraterritorial Jurisdiction Act and give the FBI authority to investigate offenses by private security contractors worldwide.

a. Would the FBI support legislation to expand its authority to hold private security contractors fully accountable for crimes committed overseas?

Response:

The FBI would be pleased to provide its views of this proposed legislation to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00113 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.086

14. While the Nisoor Square killings have drawn the most publicity, those shootings were not an isolated event. Blackwater forces have a documented history of shootings in Iraq which have resulted in civilians being seriously injured and killed. There were two other shooting incidents in the same month as the Nisoor square killings, in which five civilians were killed and fifteen more were wounded. Since 2005, there have been nearly 200 other shootings by Blackwater guards in Iraq, and in more than 160 of those incidents, the Blackwater guards fired first.

a. Other than the Nisoor Square incident, has the FBI opened any investigations into any private security contractor shootings in Iraq or Afghanistan?

Response:

The FBI has participated in three investigations of possible private security contractor shootings in Iraq. The FBI has not investigated any allegations of private security contractor shootings in Afghanistan.

b. What steps have you taken to make sure that shooting incidents by private security contractors in Iraq and Afghanistan are aggressively investigated and prosecuted?

Response:

The FBI is working closely with DOJ, DOS, and the Department of Defense (DoD) to review relevant cases in which there may be Federal criminal jurisdiction and to coordinate responses to such crimes.

Name Check Backlog

15. I am concerned that the FBI's delays in performing name checks as part of the immigration process has created an unnecessary backlog. Having name checks pending for as long as 3 years has led to some people being unnecessarily denied immigration benefits and to others who should not be in the United States remaining here and unaccounted for. When the FBI briefed congressional staff along with officials from the Customs and Immigration Service recently, we were told that both agencies were in the process of developing an action plan to resolve these delays.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00114 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.067

a. Can you tell the Committee what progress has been made on that plan and when it will be available to Members of Congress?

Response:

On 4/2/08, the FBI and U.S. Citizenship and Immigration Services (USCIS) announced a joint plan to eliminate the name check backlog. The plan focuses on resolving the oldest pending FBI name checks first. USCIS has requested that the FBI prioritize resolution of approximately 29,800 pending name checks from naturalization applicants submitted to the FBI before May 2006 in which the naturalization applicant has already been interviewed.

b. What else is the FBI doing to clear this backlog, especially in light of the enormous surge of naturalization applications the United States is currently experiencing?

Response:

The FBI's steps to reduce the pending USCIS name checks include the following.

- The FBI has hired contractors to augment the FBI staff processing USCIS requests. Currently over 200 contractors jointly funded by the FBI and USCIS are onboard and dedicated to processing USCIS name checks, with approximately 80 additional contractors to be added.

- The FBI raised fees in order to properly resource the program. Before this increase, the fees charged to process name checks had not been adjusted since the early 1990's and did not cover the basic costs of providing the service. A fee study determined an appropriate fee to offset the cost and the FBI has implemented an interim fee while the final fee structure is undergoing the "Notice of Proposed Rulemaking" process.

- In coordination with USCIS, the FBI revised the criteria used to identify unproductive searches.

- The FBI re-prioritized its workload and is now processing the oldest cases first. By focusing on the oldest cases and USCIS requests for expedited review, the backlog of USCIS name checks pending for more than four years has been eliminated.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00115 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.088

- The FBI has revamped the name check process, moving the "File Review" phase of the process (when paper files are located and scanned) from the middle of the process to the end. Because the files associated with many USCIS name checks are electronically available and do not require the retrieval of paper files, this restructuring significantly streamlines the path followed by many USCIS name checks.

- When paper files must be reviewed, the FBI is scanning these files, creating an electronic data base to which analysts have remote electronic access.

- The FBI has developed an Operational Business Plan that takes maximum advantage of the additional revenue from the revised fees and funding appropriated in FY 2008 to incorporate revised business processes these funds make possible.

- Revised processes also leverage the advantages realized by embedding USCIS employees with FBI personnel to enhance coordination.

- The FBI has begun using a forecasting model to project resource and personnel usage. This dynamic tool takes into consideration aging name checks and allows for more accurate operational predictions based on adjustments to the process.

- Through contracts, the FBI has procured additional expertise in the areas of Business Statistics, Financial Management, Information Technology, and Production/Throughput. The addition of these skill sets will greatly enhance the FBI's ability to analyze data and reports, to develop and update business forecast models quickly, to plan and develop the financial aspects of the Name Check Program, to increase the emphasis on business automation and the use of new information technology systems, and to focus on evaluating and implementing means of increasing throughput.

- The FBI is tagging records to improve our ability to retrieve and access records. This process will ease access to the information contained in billions of pages of documents.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00116 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.089

16. The Center for Human Rights and Global Justice at NYU Law School produced a report entitled "Americans on Hold: Profiling, Citizenship, and the 'War on Terror' " in April of 2007. This report examined the impact of name check delays on a number of individuals from Middle Eastern or South Asian countries. Some observers fear that after 9/11, the Federal government has been engaged in profiling people from certain parts of the world, and have argued that such profiling is not an effective way to ensure that those seeking permanency in the United States do not seek to do us harm.

a. Can you assure the Committee that the FBI is conducting name checks in an objective manner and without the use of racial or ethnic profiling?

Response:

The majority of USCIS name check requests are submitted in batches on magnetic tapes. These tapes are uploaded into an FBI computer system and the names are electronically checked against the FBI's Universal Index of names. All submitted names go through the same process, regardless of the name or the place of birth. Therefore, all names submitted by USCIS are treated in the same, objective manner.

b. Does the FBI's data showing the country of origin of applicants whose name checks have been pending for one year or more show a disproportionate impact on applicants of certain nationalities? Can you provide this data to the Committee?

Response:

The FBI does not track completed or pending name checks by country of origin.

Authority to Sign FISA Applications

17. The House and the Senate are now negotiating a bill that would make significant changes to the manner in which intelligence is gathered under the Foreign Intelligence Surveillance Act. One provision of the bill that passed the full Senate last month would permit the Deputy Director of the FBI to be the certifying official on FISA applications. The Senate Judiciary Committee's version of this bill provided that the FBI Deputy Director could not certify unless FBI Director was "unavailable." This restriction was not meant to unduly burden the delegation of this function to the Deputy Director. It was simply meant to clarify that the certifying official for FISA applications should be,

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00117 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.070

whenever feasible, a politically accountable official who has been appointed by the President and confirmed by the Senate. The bill that ultimately passed the Senate did not include this restriction. If this provision in the Senate bill is part of any final FISA legislation, would you nonetheless commit to continuing to be the certifying official on FISA applications unless you are truly unavailable to sign off on these critically important applications, which directly impact Americans' privacy rights?

Response:

The statutory authority to certify FISA applications is one the FBI Director takes very seriously. The Deputy Director would view it with equal seriousness, and the Director has every confidence in the Deputy Director's ability to exercise that authority in the proper manner. Yet, as the question suggests, it is the Director's intent to continue to perform the certification duties unless he is unavailable.

Questions Posed by Senator Kennedy

Criminal History Background Checks

In a June 2006 report to Congress on criminal history background checks, the Attorney General stated that even though the FBI's database "is quite comprehensive in its coverage of nationwide arrest records for serious offenses, [it] is still missing final disposition information for approximately 50 percent of its records." In other words, in about half of its arrest records, the FBI database doesn't show whether initial charges were dropped or the individual was acquitted.

That's unacceptable, especially since more and more employers are using FBI rap sheets to do criminal background checks on job applicants. The FBI provides about 5 million background checks a year for employment and licensing purposes. Some private employers can also obtain access to FBI records. When the records are incomplete or inaccurate, they give a distorted view of the labor market.

It's obviously unfair to job applicants. When rap sheets are incomplete, employers may never learn that an applicant was cleared of any charges. Because racial profiling is still a reality in many communities, the problem disproportionately affects African-American and Latino applicants, and employers are also more likely to penalize minorities for having a criminal record.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00118 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.071

I understand that the FBI has also proposed regulations to add "non-serious offenses" to the rap sheets. Non-serious offenses are juvenile offenses and offenses that are less than misdemeanors, such as loitering, vagrancy, and traffic violations. This change will only compound the problems caused by incomplete and inaccurate rap sheets.

18. Are you familiar with the Attorney General's report two years ago that nearly half of the arrest records in the FBI database have no information on the final disposition of the arrests?

Response:

The AG's Report on Criminal History Background Checks was prepared with input from the FBI, state repositories, the National Crime Prevention and Privacy Compact Council (hereinafter the Compact Council), professional background screeners, trade associations, private security companies, and others. The purpose of the report was to provide insight on the existing laws, regulations, policies, procedures, and standards for performing criminal history record checks. The report included recommendations for a more uniform system for obtaining FBI criminal history records for employment, licensing, and national security purposes.

Although the AG's report indicates that the FBI is "still missing final disposition information for approximately 50% of its records," it notes that "no single source exists that provides complete and up-to-date information about a person's criminal history" and that "the FBI-maintained criminal history database . . . is certainly one of the better sources. . . ." For this reason, the report recommended that entities check all available criminal history record databases, including state and local record repositories, to obtain a criminal history record that is as complete as possible.

Through the NGI initiative, the FBI has developed additional capabilities. NGI Quick-Win was delivered in July 2007, providing the ability to submit dispositions and expungements in compact disk form. The Interstate Identification Index message key was completed in February 2008, providing the ability to update dispositions electronically. These capabilities will improve the completeness of the FBI's criminal history record repository by enabling State Identification Bureaus to update criminal history records more efficiently and

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00119 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.072

quickly. The FBI will also work with Federal, state, and tribal agencies to implement the National Instant Criminal Background Check System (NICS) Improvement Amendments Act of 2007, the purpose of which is to improve the collection, automation, and transmission of criminal history dispositions and other record information.

19. Do you agree that it's important to guarantee that the FBI database is accurate and reliable?

Response:

The accuracy and reliability of the FBI database is very important. In FY 2007, the FBI processed over 11.2 million criminal fingerprint requests and over 12.7 million civil fingerprint requests. In addition, we processed over 200 million name-based Interstate Identification Index inquiries (this index provides authorized users with online access to the criminal history records of approximately 57 million subjects). FBI criminal history records are used to support the delivery of Federal, state, local, territorial, tribal, and international law enforcement and criminal justice services (including criminal identification and apprehension, homeland security, and national security), as well as noncriminal justice services (such as employment, licensing, and immigration services). The FBI is aware that our customers depend on this information to identify terrorists, to identify, prosecute, and sentence criminals, to secure our key infrastructures and critical facilities, to regulate licensed professions, and to protect our children and other vulnerable populations.

20. Has the FBI made any effort to make sure that employers receive only accurate and complete information about the criminal history of workers?

Response:

The FBI is authorized by Federal law to exchange criminal history record information (CHRI) with state and local governmental entities for noncriminal justice purposes, such as employment and licensing. In some cases, the FBI is also authorized by Federal law to disseminate records to non-governmental entities for employment and licensing purposes, such as officials of federally chartered or insured banking institutions. The officials making suitability determinations related to licensing or employment must provide applicants with

the opportunity to complete, or challenge the accuracy of, the information contained in the FBI criminal history record. Officials making suitability determinations may not deny a license or employment based on the record's information until the applicant has been afforded reasonable time to correct or complete the record, or has declined to do so. This policy is intended both to ensure that relevant CHRI is made available to those responsible for public safety and to protect prospective employees and licensees who may be adversely affected by inaccurate or incomplete CHRI. (For a fee, an individual may request a copy of his/her FBI Identification Record for personal review at any time. Since the FBI is not the primary source of data appearing on this record, however, the FBI is not authorized to modify a record without written notification from the appropriate criminal justice agency.)

21. Studies show that African-Americans are 15 times more likely than Whites to be arrested for "non-serious offenses," even though less than 20% of these arrests result in convictions. Do you agree that releasing non-serious offense records to employers will raise even greater concerns?

Response:

As discussed in response to Question 2, above, 28 U.S.C. § 534(a)(1) requires the AG to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records." Federal and state agencies are not required to provide identification information to the AG, but rather do so voluntarily. The FBI disseminates the entire criminal history record, with the exception of sealed or expunged CHRI, when it provides a match to a proper inquiry. The FBI does not establish suitability criteria, nor does it conduct suitability determinations, unless otherwise required by Federal law. Instead, the officials reviewing the CHRI are responsible for performing suitability determinations in accordance with the criteria established by the state or the affected agency.

Many states have established procedures for screening criminal history records and are prohibited from disseminating non-conviction CHRI for employment and licensing purposes. The Compact Council has established screening standards for CHRI received through the Interstate Identification Index system for noncriminal justice purposes, including the following.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00121 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.074

- The State Criminal History Record Repository or an authorized agency in the receiving state will complete the required record screening for all noncriminal justice purposes.

- An authorized official must screen the record to determine what information may legally be disseminated for the purpose for which it was requested. This record screening is conducted pursuant to the receiving state's laws, regulations, and policies.

- If the receiving state has no established laws, regulations, or policies providing guidance on the screening of the CHRI, then the record screening is performed in the same manner as the state screens its own records for noncriminal justice purposes.

22. Making employment-related background checks more accurate would not only provide fairness to the people who are affected; it would also improve the safety and security of our workforce, and help more companies meet their employment needs. When the FBI does background checks on firearms purchasers, it already looks for complete arrest records, so we know such efforts are possible. Do you agree that the FBI needs to improve the reliability of information that's distributed to employers?

Response:

The FBI recognizes the importance of basing employment and licensing decisions on accurate information, as well as recognizing the resources required to research and retrieve information pursuant to criminal history record checks. The resources required to manually retrieve CHRI from state and local agencies would increase considerably both the FBI's response time and the cost of processing fingerprints for noncriminal justice purposes.

The best way to improve the reliability of the FBI's database is to improve the thoroughness and timeliness of the reports of arrests and dispositions provided to the FBI. Currently, agencies can submit this information in various formats, including hard copy, Machine Readable Data tapes, compact disk, digital versatile disk, and e-mail.

The FBI works with the submitting agencies to identify and implement alternative methods for collecting disposition information so it can be added to IAFIS. One

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00122 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.075

such initiative allows disposition information collected during the background check process to be posted outside the requirements set forth in the single-source submission guidelines. Another initiative to increase IAFIS' accuracy and completeness involves the collection of information regarding the underlying arrest when disposition information has been submitted but there is no arrest on file. The FBI has also obtained access to some state web sites and is retrieving arrest and/or disposition information from these sites for addition to IAFIS. These proactive approaches improve IAFIS' accuracy and completeness.

In addition to efforts to improve the quality and number of arrest and disposition submissions, the FBI promotes the National Fingerprint File (NFF) Program, pursuant to which a participating state retains responsibility for maintaining and distributing its CHRI for both criminal justice and noncriminal justice purposes. The advantage of the NFF program is that participating states provide copies of their own state-maintained criminal history records in response to national criminal history record requests. Twelve states currently participate in the NFF program and more states are expected to join the program in the future.

Interrogation Practices

As you know, the nation continues to be haunted by the issue of torture. The 2002 Bybee "torture memo" by the Office of Legal Counsel defined torture in an absurdly narrow way. Along with the photos from Abu Ghraib prison, the memo caused worldwide outrage when it came to light. Just the other day, additional shocking photos from Abu Ghraib were revealed. We're still trying to learn the details of two additional torture memos issued in secret by the Office of Legal Counsel in 2005. We've learned that the CIA destroyed videotapes showing the use of abusive interrogation techniques. Both the Attorney General and the Director of National Intelligence have acknowledged that waterboarding would be torture if used against them, but they refuse to say that waterboarding is unlawful when used against others. The CIA's secret "black sites" and Guantanamo Bay continue to be symbols of the Bush Administration's hypocrisy and cruelty in the treatment of detainees.

As you testified at the hearing, the FBI has long held the view that non-coercive forms of interrogation work best. But the Administration has consistently ignored Congress and the Bureau on the issue, and its torture policies have stained America in the eyes of the world. Any day now, it's expected that the President will add insult to injury by vetoing a bill to strengthen our prohibitions against torture.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.076

The bill requires all U.S. government agencies - including the CIA - to comply with the Army Field Manual's standards on interrogation, which are consistent with the FBI's standards. As military leaders have long recognized, this approach will produce better intelligence, end worldwide outrage over our interrogation practices, and protect our own personnel from abusive treatment abroad.

23. Do you agree that the Army Field Manual's standards should be applied to all U.S. government interrogations? The Field Manual allows flexibility for interrogators, but it leaves no doubt that torture can never be used.

Response:

Speaking only for the FBI, we have some concerns about whether a manual designed for soldiers, who may be young, have limited training, and be conducting interrogations in a battlefield environment, would be appropriately applied to the FBI. We are not aware of any FBI interview technique that would be expressly prohibited by the Army's current Field Manual. Nonetheless, the FBI has a long history of conducting interviews using techniques that have been accepted by Article III courts reviewing interviews of criminal defendants. These standards could be different from those acceptable in a battlefield setting. It would be a curious result if the FBI's techniques, which have been approved by the Federal courts as constitutional and not in derogation of a criminal defendant's rights, were subject to challenge because they did not clearly fall within a category defined in the Field Manual. For example, the courts have held that it is permissible to deceive a criminal defendant. (*See, e.g., Frazier v. Cupp,* 394 U.S. 731 (1969) (defendant was falsely told that his accomplice had confessed); *Ledbetter v. Edwards*, 35 F.3d 1062 (6th Cir. 1994) (involving fake fingerprints and lies regarding witness identifications); *United States v. Velasquez*, 885 F.2d 1076 (3d Cir. 1989) (defendant was falsely told that an accomplice was cooperating with authorities).) Such deception may possibly be encompassed within the Field Manual's so-called "we know all" approach. However, as stated above, it would be unfortunate if such techniques were subjected to challenges and appeals simply because they are not explicitly listed among the Field Manual's eighteen currently approved approaches. Consequently, we believe it is inappropriate to impose military interrogation policies on FBI agents, who have both domestic law enforcement and national security missions.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00124 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.077

24. In September 2006, the Army's top intelligence officer, Intelligence Lt. Gen. John Kimmons, said: "No good intelligence is going to come from abusive practices. I think history tells us that. I think the empirical evidence of the last five years, hard years, tells us that." Do you agree with General Kimmons?

Response:

It is the FBI's policy that no interrogation of a detainee, regardless of the detainee's status (e.g., enemy combatant or prisoner of war), will be conducted using methods that could be interpreted as inherently coercive. Other than the administration of Miranda warnings, the interrogation techniques the FBI uses on detainees outside the United States are the same as would be used on criminal defendants inside this country. The FBI's experience is that our rapport-based techniques are effective and reduce the risk of obtaining a false confession from a person who is simply seeking to end the interrogation.

25. A *Washington Post* article last December reported that the FBI and the CIA have repeatedly clashed over the use of coercive interrogation techniques. In the case of Abu Zabaida, the article said, "Tensions came to a head after FBI agents witnessed the use of some harsh tactics, including keeping him naked in his cell, subjecting him to extreme cold, and bombarding him with loud rock music." The article said that you eventually ordered the FBI to withdraw from the interrogation, because Bureau procedures prohibit agents from being involved in such techniques. Is the *Washington Post*'s account of the FBI's role in the Abu Zabaida interrogation accurate?

Response:

By longstanding FBI policy, FBI personnel do not use force, threats, or promises during the course of interviews. Following the capture of Abu Zubaydah in 2002, the FBI Director determined that FBI policy regarding interrogation techniques would not change, regardless of what techniques were authorized for other agencies. The facts and circumstances related to this question were reviewed at length by the DOJ IG in the report entitled "A Review of the FBI's Involvement in and Observations of Detainee Interrogations in Guantanamo Bay, Afghanistan, and Iraq."

26. Many news stories have described a rift between the FBI and the CIA over interrogation, with the Bureau unwilling to go along with the CIA's extreme techniques

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00125 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.078

and its cavalier approach to the law. It's been reported that the FBI withdrew personnel from Guantanamo because of the abuses that were occurring at the prison camp. FBI documents have catalogued the coercive techniques used there. One FBI agent told of observing a detainee who had been shackled overnight in a hot cell, soiled himself, and pulled out tufts of hair in misery. Another agent reported seeing detainees chained from hand to foot in the fetal position for up to 24 hours.

a. Can you comment on the FBI's experience in Guantanamo - what the Bureau observed there, what role it played, how you came to withdraw your interrogators, and why?

Response:

The FBI's role in interviewing detainees and its observations at Guantanamo have been subjected to extensive review by DOJ's OIG. The IG's 5/20/08 report provides a thorough review of the FBI's observations at Guantanamo.

b. Can you comment on the rift that's been described in the media between the FBI and the CIA over interrogation techniques?

Response:

As described at length in the IG report referenced above, the FBI determined not to participate in interrogation techniques that would be inappropriate if conducted inside the United States.

c. What is your view of the CIA's so-called "enhanced interrogation program"? It clearly goes beyond any of the techniques the Bureau allows. Do you believe the CIA's "enhanced" techniques are not only unlawful, but also ineffective?

Response:

Please see the response to Question 24, above. Because FBI personnel were precluded from using any interrogation techniques that would not be appropriate for use in the United States, there has been no need for FBI employees, including the Director, to read the applicable DOJ Office of Legal Counsel opinions regarding interrogation techniques. Nevertheless, the FBI has repeatedly expressed its belief that rapport-based interrogation techniques are the most

---

These responses are current as of 6/22/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00126 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.079

effective techniques to gather reliable information from individuals being questioned.

27. What can you tell us about the progress of the FBI investigation of the interrogation videotapes destroyed by the CIA? Attorney General Mukasey has said that the FBI has a lead role in the investigation.

Response:

At the AG's direction, on 1/4/08 the FBI initiated its criminal investigation into possible obstruction of justice relative to the destruction of the interrogations tapes. A team of FBI SAs and analysts, led by an FBI Inspector, is working in conjunction with the DOJ-appointed prosecutor in charge, John Durham, and his team of attorneys. Because this investigation is pending, the FBI cannot provide details relative to its status, but we can offer that this work is ongoing and is expected to continue for some time.

28. In testimony before this Committee in January, Attorney General Mukasey was unclear on whether he would allow the investigation of the destroyed tapes to include the conduct shown on the tapes.

a. Has the Attorney General authorized the FBI to investigate the content of the tapes, not just the act of destroying them?

Response:

The AG has not specifically authorized an investigation relative to the content of the tapes. However, while the content of, or the conduct shown on, the tapes is not the focus of any investigation, such content may be considered when making a determination relative to motivation or intent into the destruction of the tapes.

b. Is the FBI investigating whether the conduct shown on the tapes is torture?

Response:

The focus of the investigation is potential obstruction of justice regarding the destruction of the videotapes. While the content of the tapes, or the conduct

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00127 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.080

shown on them, is not the focus of any investigation, it may be considered when making a determination regarding motivation or intent with respect to the destruction of the tapes.

c. Will you make a public commitment that, to the extent you have the authority to do so, you will permit your investigators to look into the conduct shown on the tapes?

Response:

The AG will determine, based on the facts of the investigation, whether the scope of the DOJ/FBI investigative will be expanded to include a review of the conduct shown on the tapes.

29. Have you taken any steps to decide whether investigations of other possible past acts of torture are needed? Have you considered whether an FBI investigation is needed for interrogations at Guantanamo?

Response:

As the AG suggested in his 1/30/08 testimony before this Committee, and as Principal Deputy Assistant AG Benczkowski emphasized in his 4/22/08 correspondence to this Committee, it is the AG's position that the Department will not investigate any conduct that was undertaken in reliance on the Department's past legal advice.

Consistent with long-standing AG Guidelines, the FBI cannot open an investigation unless there is some factual basis on which to do so (generally this is information regarding, or allegation of, criminal conduct). In the context of interrogations conducted by the CIA, the CIA IG has conducted one or more reviews of the CIA program. Pursuant to existing Memoranda of Understanding and AG Guidelines, if the CIA IG had discovered evidence of criminal conduct, he would have been obligated to report that conduct to the FBI for investigation. Moreover, following the transfer of high-value detainees who had been in CIA custody to Guantanamo, the FBI, CIA and DOJ agreed on a process by which detainee allegations of abuse would be handled. Pursuant to that letter of understanding, the FBI reported all detainee allegations of mistreatment to the Inspector General of the CIA, with a copy to the CIA General Counsel and the

U.S. Attorney's Office for the Eastern District of Virginia (EDVA). If the allegations involved treatment beyond the scope of that authorized, the agreement required the CIA Inspector General to report that fact to the U.S. Attorney's Office and an investigation would then proceed.

In August 2005, the FBI referred one matter involving alleged detainee abuse, and the FBI was advised by EDVA on 3/8/07 that the matter had been declined for insufficient evidence. Between February 2007 and August 2008, consistent with the letter of understanding, the FBI referred additional allegations of detainee abuse to the CIA OIG. We understand that these are currently under consideration by the CIA IG.

At this time, the FBI has no information that any CIA employee or contractor used interrogation techniques that were not within the scope of the authority they had been given. In light of that, the FBI does not have adequate predication to open a criminal investigation. Should that situation change (that is, if the FBI should learn of information, based on existing FBI investigations, CIA IG investigations, or otherwise, suggesting that CIA interrogations exceeded the scope of authorized activity), the FBI would investigate any information received to its logical conclusion.

In the context of interrogations conducted at Guantanamo, consistent with existing agreements between DOJ and DoD, the FBI referred all instances of abusive or arguably abusive treatment of detainees known to the FBI to DoD for its consideration. As you know, DoD has jurisdiction over the armed forces under the Uniform Code of Military Justice.

DoD assigned the responsibility of investigating those matters to Lieutenant General Randall Schmidt and Brigadier General John T. Furlow. The Schmidt-Furlow report, which was issued in early 2005, found that certain activities reported by FBI agents were not authorized and recommended that command action be taken with respect to the responsible parties. Other activities reported by FBI agents were either found to be authorized, to be unauthorized but lacking adequate information to determine the responsible party, or to be unsubstantiated. Generals Schmidt and Furlow specifically investigated the techniques used during the interrogations of Muhammad Al-Qahtani and Mohamedou Slahi.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.082

30. In a recent study entitled "Captured on Tape: Interrogation and Videotaping of Detainees in Guantanamo," Professor Mark Denbeaux and colleagues used publicly available documents to examine interrogation practices at Guantanamo. They found that: (1) the FBI is one of many entities that has interrogated detainees at Guantanamo; (2) more than 24,000 interrogations have been conducted at Guantanamo since 2002; (3) every interrogation conducted at Guantanamo was videotaped; (4) the government kept meticulous logs of information related to interrogations at Guantanamo, so we know which videotapes documenting interrogations still exist, and which videotapes have been destroyed; and (5) any videotapes that still exist are in danger of being destroyed.

a. Is each of these five statements accurate?

b. What steps has the FBI taken to make sure that all videotapes of interrogations at Guantanamo are preserved?

c. Will you commit to doing everything in your power to see that all of these videotapes, known and unknown, are preserved?

Response to subparts a through c:

The FBI is one of several agencies that has interviewed detainees at Guantanamo. Following the revelation that a CIA employee had destroyed videotapes of interviews of high-value detainees, the FBI began an investigation of that conduct. Beyond the information being obtained through that investigation, the FBI is not aware of the total number of interviews conducted at Guantanamo, we are not in possession of logs created there, and we are not aware of any interview videotapes in the possession of other agencies. While the FBI is aware that some interviews at Guantanamo were videotaped, this videotaping was not accomplished by the FBI or at the FBI's request.

In connection with the investigation referenced above, the FBI has received a grand jury subpoena that seeks videotapes of certain categories of detainee interviews. As a matter of policy, the FBI has decided to preserve all videotapes of detainee interviews, regardless of where they occurred and regardless of whether they are responsive to the grand jury subpoena. We have, therefore, collected and are safeguarding these tapes.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.083

d. Do you think all detainee interrogations should be videotaped? What is the official FBI policy on this question?

Response:

While the FBI's general policy is not to videotape interviews, this policy is subject to certain exceptions. This approach is the same one taken with respect to the electronic recording of confessions and witness interviews, which is not generally done but is permitted when authorized by the Special Agent in Charge (SAC) or his or her designee. Similarly, while FBI policy generally precludes the videotaping of detainee interviews outside the United States, exceptions can be made.

The FBI does not have a position on whether other agencies should videotape detainee interviews.

e. If you believe that any of the information needed to respond to the previous four questions is classified, will you commit to providing your answers to the Committee in a classified setting?

Response:

Please see the above responses to the four questions referenced.

Questions Posed by Senator Feingold

32. You assured me at the hearing that you would check on the status of the report due to Congress under the Federal Agency Data Mining Reporting Act. That law, which was enacted last summer, requires that all data mining programs for counter-terrorism or criminal purposes be reported to Congress. The first set of reports was due in January.

a. When can we expect that report?

b. Will the report include information about NSAC, and if not, why not?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.084

Response to subparts a and b:

Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No. 110-53) requires the heads of all Federal agencies to submit an annual report regarding the organization and operations of every program engaged in "data mining," as defined in the statute. As a DOJ component, information concerning FBI programs is included in the report submitted by DOJ.

33. You testified before the Committee that "[i]n the wake of September 11th, [the FBI] had to move 900 agents from drug programs over to national security." You also stated that "as a result of what happened on September 11th, [the FBI is] not participating in addressing the drug problem in this country as we were prior to September 11th. We do it in the context of addressing gangs and violent crime ...." Please answer the following questions:

a. How is the FBI currently addressing the drug problem in the context of gangs and violent crime? Please elaborate on what types of cases fall outside the scope of the FBI's work.

Response:

The FBI's Safe Streets Violent Crimes Initiative was established in 1992 to attack gang and drug-related violence through the establishment of long-term, proactive, coordinated teams of Federal, state, and local law enforcement officers and prosecutors. As a result of this initiative, the FBI's VGSSTFs were established to identify and target violent street gangs, outlaw motorcycle gangs, and prison gangs as criminal enterprises. Most, if not all, FBI gang investigations have a nexus to drugs and/or violent crime. Currently, the FBI operates 143 VGSSTFs (with 1,243 TFOs) and 41Violent Crime Safe Streets Task Forces (with 282 TFOs).

The FBI's VGSSTFs pursue violent gangs through investigations focused on racketeering, drug conspiracy, firearms, and related offenses. The FBI uses the Safe Streets Task Force (SSTF) concept to address the drug problem in the context of gangs and violent crime. As the majority of drug trafficking in the United States involves gang and other violent crime activity to one degree or another, the FBI addresses the drug problem through SSTF operations, which increase productivity, minimize the duplication of investigative efforts, and

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00132 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.085

expand cooperation and communication among Federal, state, and local law enforcement agencies.

One of the key facets of an SSTF operation is the Enterprise Theory of Investigation (ETI). Combining short-term, street-level enforcement activity with sophisticated investigative techniques, such as consensual monitoring, financial analysis, and Title III wire intercepts, investigations using ETI work to root out and prosecute entire gangs, from street-level thugs and dealers, up through crew leaders, and ultimately including the gang's command structure. For the past 14 years, the ETI has relied on Federal racketeering and drug conspiracy prosecutions to effectively disrupt and dismantle criminal enterprises involved in the drug trade.

While drug cases with no apparent connection to gangs or other organized crime generally fall outside the scope of the FBI's work, the FBI has maintained a presence in certain drug intelligence operations, such as the Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center, the El Paso Intelligence Center, and the Special Operations Division. In addition, the FBI has served in a leadership role with respect to Operation Panama Express (PANEX). PANEX South is managed by an FBI SA and the FBI provides operational, administrative, and technical support to this interagency group.

b. How did the Bureau address the drug problem before September 11th? What sort of issues was the Bureau tackling regarding the nation's drug problem prior to September 11th that it no longer is addressing?

Response:

Before the terrorist attacks of 9/11/01, the FBI had a section dedicated to disrupting and/or dismantling criminal enterprises involved in the illicit drug trade, including their money laundering operations. These efforts were clearly aligned with the national priorities of the Consolidated Priority Organization Target list and its predecessor, the National Priority Target List. These lists detail Drug Trafficking Organizations identified by Federal, state, and local law enforcement entities as being the most significant targets for investigation. The FBI targeted large national and international drug trafficking organizations and individuals assisting these organizations, using the ETI to target subjects in criminal enterprises, including national and international leaders, money

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00133 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.086

laundering organizations, and street-level dealers. Since 09/11/01, the FBI has targeted domestic drug trafficking organizations, primarily through participation in OCDETF operations and through our 143 VGSSTFs.

c. To your knowledge, are these issues now being addressed by the DEA?

Response:

It is the FBI's understanding that the Drug Enforcement Administration (DEA) continues to address both national and international drug trafficking organizations.

34. One of the ways that states and local governments are able to battle violent and drug-related crime is through the Byrne Justice Assistance Grant program. The current administration, however, has sought to reduce or even eliminate funding for Byrne grants for several years, as exemplified by the President's proposed budget for fiscal year 2009. In Wisconsin, the cuts in Byrne funding are increasingly devastating. It means fewer prosecutors, fewer officers, and fewer resources to deal with the rise in violent crime. At the federal level, you noted a resource shift of 2,000 FBI agents to national security matters and away from more traditional domestic criminal matters since September 11th.

a. Given the FBI's shift away from traditional criminal matters, states and local agencies are being asked to shoulder an increasing burden in the fight against violent crime. Wouldn't a reduction in Byrne funding compound this problem?

Response:

The FBI is not involved in funding decisions for Byrne/Justice Assistance Grant programs and defers to DOJ with respect to this inquiry.

b. There were significant increases in violent crime starting in 2005. Is it prudent to propose a reduction in federal grant funds to state and local law enforcement aimed at fighting violent and drug-related crimes, as the President's budget proposal does?

Response:

The FBI works with DOJ and the Office of Management and Budget (OMB) to develop the President's budget proposal.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00134 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.087

35. Many of the programs that may have to be cut due to a reduction in federal crime-fighting grant funds are focused on crime prevention and intervention efforts to reduce the number of repeat offenders. These prevention and intervention programs are critical to reducing crime. Are you concerned about the reduction in crime prevention and intervention programs?

Response:

The FBI recognizes that many factors may influence crime levels. As a law enforcement agency, our primary focus is on enforcement efforts.

36. Recently, the Inspector General of the Justice Department issued a report finding that the FBI is chronically late in making payments to telecommunications companies for implementing wiretaps. According to the public version of the IG report, more than half of the audited payments were late, and "late payments have resulted in telecommunications carriers actually disconnecting phone lines established to deliver surveillance results to the FBI, resulting in lost evidence." The IG also said this problem resulted in disruption of a foreign intelligence wiretap required by a FISA order. You testified that in two instances a wiretap was cut off due to bill payment issues, but that neither adversely affected the investigation.

a. What assurances can you provide confirming that this problem only occurred twice and did not negatively impact any investigation? Please provide any relevant materials.

Response:

The FBI ordered a review of the two cases in which the OIG report identified interrupted FISA wiretaps due to nonpayment, finding that the impact of the surveillance interruptions on these cases was negligible either because the information was recovered or because additional surveillance was in place. Surveillance interruptions due to nonpayment are extremely rare, and the risk of losing evidence because of an interruption due to nonpayment is even more remote. Improvements in the FBI's processes and internal controls, both before and in response to the OIG's recommendations, have further reduced this risk.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00135 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.088

b. How did such lapses occur in the first place, and what remedial steps has the agency taken to prevent this from happening in the future?

Response:

Please see the response to Question 4, above.

37. As the result of a FOIA request, an internal FBI email from June 2006 was released last year suggesting that FBI agents have pressed communications service providers to hand over information without a court order. A copy of the email is attached. The email states: "Getting a court order is the absolute last step, if they have to."

a. Are you concerned about the allegations in this email?

Response:

Although the FBI takes these types of comments seriously, all Wireless Intercept Tracking Team (WITT) members are already appropriately trained in the operational, procedural, and legal requirements for using this technology. WITT Agents and other FBI personnel are instructed to seek issuance of a court order (unless an exception is applicable, such as consent by the subscriber or pursuant to subpoena) before deploying WITT equipment or asking a communication service provider to provide cell site information. Our confidence in the training and procedures in place concerning these types of investigative techniques minimizes any concerns about the allegations in this email.

b. As a result of this email, has the FBI investigated whether agents have been improperly obtaining or trying to obtain communications records without a court order?

Response:

A court order is not always a legal prerequisite to the disclosure of communications records. Records may also lawfully be disclosed by a provider voluntarily in an emergency, pursuant to consent of the subscriber, pursuant to subpoena, or under other circumstances not involving a court order. As indicated in response to subpart a, above, WITT Agents and other relevant employees are trained in the proper procedures for deploying WITT equipment or requesting cell

site information from communication service providers. A website managed by the FBI's Operational Technology Division provides examples of orders and affidavits to assist case Agents in obtaining the appropriate court orders. When FBI Agents are assisting state and local law enforcement, established FBI procedures require coordination with the local jurisdiction before the FBI assists in the WITT mission.

c. What action, if any, would be taken against agents found to have pressured communications companies into releasing information without a court order?

Response:

As indicated above, although we take all allegations of this nature seriously, we note that the statements do not necessarily suggest that any provider was inappropriately pressured into releasing information without a court order. As also noted above, there are other lawful processes - not involving the issuance of a court order - under which a service provider may disclose information (for example, a communication service provider may provide information voluntarily without a court order in emergency circumstances pursuant to 18 U.S.C. § 2702(c)(4)). The FBI maintains close relationships with communication service providers, and there is no indication that these providers are being pressured to provide information without appropriate legal process. If the FBI suspects any employee is pressuring a communication service provider to provide information in violation of law or policy, the appropriate administrative inquiry would be initiated.

d. What checks do you have in place to make sure agents do not undertake such practices?

Response:

The FBI has policy in place and provides training for Agents involved in WITT missions regarding these and a variety of other legal issues. The FBI's Operational Technology Division meets with communication service providers on a regular basis to discuss this activity, including policy and legal issues related to electronic surveillance. Communication service providers typically raise any pending issues or concerns during these meetings.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00137 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.090

38. As we discussed at the hearing, government officials, as well as declassified documents issued in response to a FOIA request, have recently confirmed that both the CIA and the Pentagon have issued National Security Letters (NSLs) to obtain financial records from financial institutions here in the United States. Please answer the following questions regarding the collection of intelligence on Americans by agencies other than the FBI:

a. You testified at the hearing that intelligence agencies needing information on Americans usually ask the FBI for assistance. You also testified that for these other agencies, "it's probably a very narrow basis for the use of national security letters." But NSL statutes covering financial records and credit reports, found in 12 U.S.C. § 3414 and 15 U.S.C. § 1681v, respectively, have provisions allowing a "Government authority" or "government agency" authorized to conduct intelligence or terrorism investigations to obtain such records for the purpose of such investigations. In light of these statutory authorities, please respond to this question: What role should the CIA and military intelligence play with respect to domestic intelligence-gathering operations, and specifically with respect to issuing NSLs? To your knowledge, what role do they play?

Response:

EO 12333 permits certain domestic intelligence collection activities by the CIA and DoD. In addition, certain NSL statutes permit the collection of information by agencies other than the FBI for national security purposes. Although Congress has authorized the FBI to issue NSLs that are compulsory, NSLs issued by other agencies, such as the CIA and DoD, are not compulsory (with the exception of NSLs issued pursuant to 15 U.S.C. § 1681v). In other words, these other agencies can make the requests, but the receiving institutions are not obligated to respond.

As we have previously advised, the FBI does not play a role in the use of NSLs by either the DoD and its component agencies or by the CIA. Any questions about the use of NSLs by the CIA or DoD should be addressed directly to those agencies.

b. Do you have any concerns about a situation in which the CIA or the Defense Department might issue an NSL to the same financial institution that the FBI works with regularly?

These responses are current as of 6/22/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00138 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.091

Response:

Section 1.8(a) of EO 12333 requires the CIA to coordinate its "collection of foreign intelligence or counterintelligence within the United States . . . with the FBI as required by procedures agreed upon by the Director of [National] Intelligence and the Attorney General." Similarly, section 1.11(d) of EO 12333 requires DoD to coordinate its "counterintelligence activities . . . within the United States . . . with the FBI pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General." The procedures required by EO 12333 are designed to ensure appropriate deconfliction of activities by these agencies and to protect appropriately the privacy and civil liberties of Americans.

c. In your view, might these potential coextensive authorities create confusion for the institutions that might receive overlapping requests?

Response:

The FBI believes the obligation to coordinate found in EO 12333 is important in ensuring that counterintelligence activities and foreign intelligence collection that occur inside the United States are appropriately deconflicted.

d. Does the FBI provide any legal input, or get notice, when other agencies like the CIA or Defense Department issue NSLs to obtain information on Americans?

Response:

As indicated above, the CIA and DoD are generally obligated to coordinate their domestic activities with the FBI. As part of that coordination process, the FBI may receive notice of their collection activities, but FBI does not provide legal advice to the CIA or DoD.

In some instances, the FBI may issue NSLs in the context of an investigation conducted jointly with other agencies. The FBI will issue such NSLs only if the information sought is relevant to an open FBI investigation and only in accordance with FBI policy and procedures.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00139 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.092

39. Last year, the FBI conducted its own internal audit of its use of NSLs. According to FBI officials that audit resulted in conclusions very similar to those of the DOJ Inspector General, which found serious problems with the FBI's implementation of the expanded authority it had been granted under the Patriot Act to use NSLs. Please provide this Committee with a copy of the FBI's audit.

Response:

The FBI's Inspection Division continues to work to finalize the report of the 10% internal audit of national security investigative case files. A large part of this report focuses on the number of deficiencies found during the audit. Though the report has not yet been finalized, the FBI is making substantial progress in addressing deficiencies, identifying "best practices" and using guidance that has been provided to the affected Divisions to address systemic issues.

40. Recently, increased attention has been paid the issue of so-called homegrown terrorism: people who have no ties to foreign terrorist organizations but become radicalized on their own. However, a Pew Research Center study concluded last year that the United States does not face the more widespread problems that Europe has in this regard. The increased focus on this issue has raised a number of concerns: that it could be used to justify racial profiling and unwarranted interference in the lives of innocent Muslim and Arab Americans, and that it could result in people being persecuted for their ideas rather than their actions. It could also serve to further alienate Muslim and Arab communities, making them less likely to cooperate with government officials. Please answer the following questions relating to the FBI's efforts on this issue:

a. What actions is the FBI currently taking to monitor and combat the prospect of homegrown terrorism? How are these actions tailored to meet specific, rather than generalized, threats, and what precautionary measures are taken to ensure that individuals are not racially profiled?

Response:

The FBI is cognizant of the threat posed by "homegrown terrorism." Longstanding DOJ policy generally precludes the FBI from commenting on the existence or status of ongoing investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence,

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00140 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.093

witness tampering, or other activity that would impede an FBI investigation. We can offer, though, that the FBI responds to all such threats within the framework established by United States laws, Federal court decisions, AG Guidelines, and FBI policies. By doing so, the FBI acts within the parameters established by these authorities to fulfill its dual missions of protecting the United States from terrorist attack while simultaneously protecting the civil rights of American citizens.

b. Do you agree that the FBI should focus its efforts on actual evidence of terrorism plots, and that a generalized concern about the possibility of homegrown terrorism does not justify widespread surveillance of Muslim and Arab communities in the United States?

Response:

The FBI does not predicate any investigation upon a "generalized concern" about any segment of our population, nor do we conduct "widespread" surveillance of any community based upon its racial or ethnic composition. Instead, the FBI focuses its efforts in counterterrorism matters on what are deemed to be legitimate threats of terrorism activity. However, the use of the word "evidence" in this question is more appropriate in the context of the high judicial standard of admissibility for information used in court proceedings than in the context of information used to identify terrorism threats at the earliest stage of consideration. While the FBI may investigate threats of terrorism or criminal activity before "evidence" has been collected, all FBI investigations must be conducted in accordance with United States laws, Federal court decisions, AG Guidelines, and FBI policies.

c. Will you ensure that the FBI will seriously consider the racial profiling and First Amendment concerns that have been raised about this issue, and work closely with the communities most likely to be affected? Please discuss your plan to address these concerns.

Response:

With respect to racial profiling, both DOJ and the FBI have already prohibited any unconstitutional or otherwise illegal consideration of race in the FBI's law enforcement decisions. Similarly, both AG Guidelines and FBI policy prohibit the predication of investigative activity solely on activities protected by the First

Amendment. Depending on the type of investigation initiated (for example, terrorism, narcotics, public corruption, or fraud), an approval and review process is employed to ensure that each investigation meets the requirements of applicable laws, guidelines, and policies, including these prohibitions.

d. Just last fall, the Los Angeles Police Department announced – and then later retracted, after public protest – a plan to collect data and map the area's Muslim community. Last summer, the New York Police Department released a report suggesting that a number of unremarkable, innocuous and non-criminal behaviors – and in particular, religious behaviors – can be the markers of someone who is on the road to radicalization. The report did not address the scores of cases in which the same conduct is not evidence of any wrongdoing or intent to commit wrong-doing. What steps is the FBI taking in its work with state and local law enforcement agencies, through task forces and other partnerships, to ensure that the increased focus on homegrown terrorism does not result in unjust adverse effects on Muslim and Arab communities?

Response:

As part of the task force agreements with state and local law enforcement agencies, all individual members of FBI task forces must agree to operate within the same laws and policies as the FBI in the conduct of investigations. This would preclude any unconstitutional or illegal consideration of race or ethnicity in law enforcement decisions, as well as the predication of investigations solely upon activities protected by the First Amendment. The investigations initiated and conducted by FBI task forces are subject to the same review and approval process applied to similar FBI investigations.

41. The FBI is launching a $1 billion effort to build a computer database of Americans' biometric data, such as facial features, ear lobe shapes, and iris patterns.

a. A major concern about this planned database is that the technology required to create, store, and match many of these kinds of biometrics is just not that advanced. Facial recognition technology, for example, is certainly not accurate enough to be relied upon for purposes of identification in a law enforcement context. I understand that the database is in the planning phase and that these technologies may become more accurate in the future, but using a biometrics database that generates significant numbers of false positive matches could result in massive disruption to innocent people's daily lives.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00142 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.095

Will you ensure that the FBI implements an appropriate accuracy requirement before relying on this database?

Response:

The FBI continues to invest in improving its biometric identification technologies in order to provide the most reliable information possible for use in law enforcement and counterterrorism efforts. Fingerprint identification is a highly reliable and widely accepted means of biometric identification, and will continue to be relied on by the FBI as an accurate means of identification. Although fingerprint data will remain the primary means of identification, the NGI initiative will assess the viability of other biometric modalities and explore if it is beneficial to advance the collection of additional biometric information for investigative purposes. While there are no formal plans to incorporate ear lobe shapes as a biometric modality, the FBI will consider this and other technologies as they mature. The NGI development and integration contract includes a series of biometric capability analyses that will assess biometric technology and provide recommendations for implementation. Issues related to research, development, testing, and evaluation that are identified through these studies will be included in the prioritization and coordination activities of the interagency National Science and Technology Council's Subcommittee on Biometrics and Identity Management. The NGI will provide the framework for the fusion of these additional biometric modalities into a highly accurate identification system.

The results achieved with all investigatory tools must be viewed using a certain "confidence interval" and with full recognition of the circumstances in which they are being used. These tools are no exception, and must also be used with those considerations in mind.

b. The privacy and security implications of this database are significant. Identity theft, for example, becomes exponentially more problematic when dealing with the theft of iris scans and fingerprints, as opposed to credit cards and bank statements. A victim of identity theft can always change his or her credit card number, but it is impossible to change one's fingerprints. What security measures will be in place for this database, and can you guarantee that they will work?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00143 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.096

Response:

Title 28 U.S.C. § 534 and 28 C.F.R. §§ 20.33 and 50.12 require that records be used only for authorized purposes and that the exchange of records is subject to cancellation if dissemination is made outside the receiving departments or related agencies. In addition, security and privacy protocols are addressed in the CJIS Division's Security Policy, to which all users must adhere.

According to Federal Information Processing Standard (FIPS) 199, systems and information are to be assigned a security categorization according to the security objectives of confidentiality, integrity, and availability. FIPS 200 establishes the minimum security requirements covering seventeen different areas for these systems, and NIST [National Institute of Standards and Technology] 800 53 was developed to provide the minimum security controls and assurance requirements according to the impact level of the data it will be processing. This database meets these minimum requirements, sitting within a system architecture that has been specifically engineered to support the security of this particular system and the rest of the FBI's CJIS systems. In addition, numerous other controls have been instituted based on industry standards and best practices.

Internally, an Information System Security Officer, who is responsible for ensuring that operational security is maintained on a day-to-day basis, has been assigned to IAFIS. The roles and rules are tested as part of the security certification and accreditation process, and all users are required to acknowledge "Rules of Behavior" in writing annually as part of security awareness training. The CJIS Computer Security Incident Response Capability also defines processes and procedures for responding to computer and data misuse concerns, and CJIS User Agreements and Outsourcing Standards provide for security and privacy to ensure compliance.

To ensure IAFIS security policies are fully implemented, the CJIS Division's Audit Unit visits authorized recipients on a recurring basis and reports deficiencies to the CJIS Division Advisory Policy Board's (APB) Sanction Subcommittee and the Compact Council's Sanctions Committee. Access may be terminated for improper access, use, or dissemination of records obtained from the system of records. The Audit Unit also conducts periodic external audits to assess and evaluate compliance with the terms of the applicable user agreements and contracts.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00144 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.097

Finally, as discussed in response to Question 3, above, 28 C.F.R. §§ 16.30-16.34 establish alternative procedures for the subject of an FBI identification record to obtain a copy of his or her own record for review and correction.

c. What would the FBI's course of action be in the case of a security breach, given that it's not possible for a person to simply replace a stolen biometric with new data?

Response:

OMB has provided clear direction and requirements for handling Personally Identifiable Information and responding to breaches. Memorandums M-06-16 (Protection of Sensitive Agency Information) and M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information) provide the required processes and procedures. DOJ has implemented these OMB guidelines for its component agencies in its own directive. When a data breach occurs in the FBI, established policy requires the FBI's Security Division and Chief Privacy Officer to jointly assess the risk of the data's exposure, its sensitivity, and the presence or absence of mitigating factors (such as data encryption). Based on this assessment, a determination is made whether to take any of a list of corrective actions, including notice to affected individuals. In addition, lessons learned about system integrity and policy effectiveness are evaluated and changes are made if appropriate.

With respect to CJIS systems in particular, an FBI audit unit visits authorized recipients periodically and reports deficiencies to the CJIS APB's Sanctions Subcommittee and the Compact Council's Sanctions Committee. If recommended by the sanctioning body, such audits may include additional biometric data. Access may be terminated for the improper access, use, or dissemination of records obtained from the system of records.

d. According to the Assistant Director of the FBI's Criminal Justice Information Services Division, the fingerprints that the FBI currently retains in its database are those belonging to people of law enforcement interest, such as criminals. When an entity or agency submits to the FBI a set of fingerprints that do not fall into that category, those prints are generally destroyed after being matched against the FBI's data. As I understand it, however, the FBI is working to implement a "rap-back" service, under which, at the request of an employer, the FBI would keep employees' fingerprints in the

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00145 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.098

database so that if that employees are later arrested or charged with a crime, the employers could be notified. This would constitute a dramatic expansion in the degree and nature of the federal government's retention of biometric data. What evidence exists that undisclosed criminal conduct among employees is a sufficiently urgent problem to justify this step?

Response:

The NGI Rap Back Service was developed because numerous states have identified a growing need for additional security and safety procedures for applicants who hold positions of trust. For example, many states have recently enacted statutes requiring fingerprints and criminal background checks for all school employees and others who have contact with children. The school-safety effort grew out of concerns related to teachers who had been arrested on suspicion of having inappropriate sexual contact with children. Because employees' aliases can thwart background checks based on names, fingerprints are widely viewed as the best means of identifying those who have incentives to falsify their identities. This danger was recently highlighted when school officials learned that a sex offender employed as a middle school custodian had passed a background check using a false name. Many states require fingerprints from new teachers, but this law does not address teachers who are already certified. Research of the 2004-05 school year indicated that in one state school system 66 teachers were registered sex offenders. In response, that state implemented a new law requiring all teachers to submit fingerprints and undergo criminal background checks. Since those checks began, state officials have advised that the records of almost 200 teachers and teaching candidates have included serious offenses, including sexual misconduct and crimes against children. Rap Back functionality will provide significant additional protection against those who violate their positions of public trust.

42. The U.S. Sentencing Commission has concluded that the statutory disparity in sentencing between crack and powder cocaine offenses has the effect of diverting law enforcement resources to low-level, non-violent drug offenders – exactly the type of cases that the FBI is no longer prioritizing, according to your testimony. Do you agree with the Sentencing Commission that Congress should reform the cocaine sentencing laws to target violent offenders and those higher up in the drug distribution chain?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00146 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.099

Response:

The FBI supports tough sentences for violent offenders involved in drug trafficking or distribution. As noted above, the FBI uses the ETI to disrupt and dismantle criminal organizations. The ETI is designed to root out and prosecute the entire enterprise, from street level dealers, up through crew leaders, and ultimately including the organization's command structure. DOJ is still developing its policy regarding narcotics sentencing laws.

Questions Posed by Senator Durbin

Human Rights

45. After the 9/11 terrorist attacks, this Administration decided to set aside our treaty obligations and to use interrogation techniques, such as waterboarding, which are inconsistent with American values and law. For decades, the FBI has been considered the nation's leading interrogation experts. As you said during a recent hearing of the Senate Select Committee on Intelligence, "Our policy has been fairly clear, from as long as certainly I've been there, and that is we do not use coercive techniques of any sort in the course of our interrogations." During his confirmation hearing, Attorney General Michael Mukasey said he would review the interrogation techniques authorized by this Administration. [The] Attorney General promised me that he would "consult with those attorneys and individuals who can provide substantive advice" on interrogation techniques.

a. In the course of his review of interrogation techniques, did Attorney General Mukasey consult with you or anyone else at the FBI?

Response:

The FBI refers you to the AG for information regarding his review of interrogation techniques.

b. What is your opinion of waterboarding, an interrogation technique that for decades the United States has repudiated and prosecuted as a war crime?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00147 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.100

Response:

Please see the response to Question 26c, above.

46. In your testimony, you spoke at length about the FBI's international operations. You said that the FBI now has Legal Attaché offices in more than 70 cities around the world. FBI agents who work in these offices are civilians; they are not uniformed personnel in the Armed Forces, so they are not entitled to Prisoner of War protections. They are however protected by Common Article 3 of the Geneva Conventions. If an FBI agent were taken hostage by a terrorist organization in a foreign country and subjected to waterboarding, would you consider this to be illegal?

Response:

Pursuant to 18 U.S.C. § 1203, regardless of whether the agent were subjected to waterboarding, if the hostage-taking were to compel a third-party or a governmental organization to do or to abstain from doing something and those actions were an explicit or implicit condition for the hostage's release, such hostage-taking would violate United States law. Both the hostage-taking and the waterboarding would also violate 18 U.S.C. § 112 regarding the "[p]rotection of foreign officials, official guests, and internationally protected persons" (terms that are defined in 18 U.S.C. § 1116). Additionally, we believe that, in every country to which we have assigned a Legal Attaché, hostage-taking would violate local law. As to whether waterboarding would violate Common Article 3 of the Geneva Conventions, we defer to DOJ and others who would be responsible for conducting the legal analysis to determine what is or is not permissible under the Geneva Conventions.

47. In response to a written question I submitted following the last Senate Judiciary Committee FBI oversight hearing, you said that since 2001, the FBI had opened seven investigations into alleged violations of the War Crimes Act and that four of these investigations remained open.

a. What is the status of the four investigations into alleged violations of the War Crimes Act that remained open last year?

These responses are current as of 6/23/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00148 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.101

Response:

The prior FBI response referenced in the question requires clarification.

The FBI organizes its investigative records by "Case Classification." Case Classification 309 encompasses three separate categories of human rights offenses: 309A is for genocide investigations (18 U.S.C. § 1091); 309B is for torture investigations (18 U.S.C. § 2340); and 309C is for war crimes investigations (18 U.S.C. § 2441). In our previous response, the FBI provided data reflecting the entire 309 classification rather than limiting our response to War Crimes Act investigations. After additional research, we can provide the following information regarding each category of offense.

No 309A (genocide) investigations have been opened since 2001. The FBI has opened seven investigations under 309B (torture) since 2001, three of which have been closed and four of which remain open as of 8/28/08. The FBI has opened three investigations under 309C (war crimes) since 2001, two of which have been closed and one of which remains open as of 8/28/08. The open 309C war crimes investigation involves alleged crimes in the former Yugoslavia, with trial ongoing in the International Criminal Tribunal.

b. Has the FBI opened any new investigations into alleged violations of the War Crimes Act since then?

Response:

Since the FBI Director's testimony in 2007, the FBI has not opened any new investigations regarding alleged violations of the War Crimes Act (18 U.S.C. § 2441).

Detainee Abuse Cases

48. I have exchanged a number of letters with the Justice Department over the last two years regarding their handling of detainee abuse allegations. In February 2008, the Justice Department informed me that of the 24 detainee abuse cases that had been referred to the United States Attorney's Office for the Eastern District of Virginia to date, 22 had been closed and only two were still ongoing. While the Defense Department has prosecuted numerous military personnel for detainee abuse, only one civilian has been convicted of

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.102

detainee abuse since 2001 and there have been no indictments since then Attorney General John Ashcroft assigned all detainee abuse cases to the United States Attorney's Office for the Eastern District of Virginia. In a January 2007 letter, the Justice Department noted that one detainee abuse case at Guantánamo had been referred by the FBI.

a. Is the case involving an allegation of detainee abuse at Guantánamo that the FBI referred to the Justice Department still ongoing?

b. Has the FBI made additional detainee abuse referrals to the Justice Department?

c. How many investigations into alleged detainee abuse has the FBI opened?

d. How many of these investigations are still ongoing?

e. How many of these investigations have been closed and why were they closed?

Response to subparts a through e:

The FBI referred one Guantanamo-related case to the U.S. Attorney's Office for the Eastern District of Virginia (EDVA), which is DOJ's office responsible for this aspect of detainee matters. The EDVA declined prosecution.

Neither the EDVA nor the FBI's Washington Field Office, which would assist the EDVA with any related investigations, currently has any pending detainee abuse cases referred by the FBI.

53. The number of hate crime incidents in America increased 7.8% -- from 7,160 in 2005 to 7,722 in 2006 -- according to the FBI's latest *Hate Crime Statistics* report. What steps, if any, has the FBI taken to address this recent rise in hate crimes?

Response:

According to the Hate Crime Statistics Act of 1990, a hate crime is a criminal offense against a person or property motivated in whole or in part by the offender's bias related to race, religion, disability, ethnic/national origin, or sexual orientation. For a hate crime to be considered a Federal criminal violation, three

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00150 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.103

elements must be present: there must be a threat or use of force, the crime must be motivated by one of the aforementioned biases, and there must be interference with a Federally protected activity. The Hate Crime Statistics report is a compilation of state and local hate-related incidents that may or may not constitute Federal hate crimes. In addition, variations in hate incident reporting among the states affect the data. For these and other reasons, the statistics reflected in that report do not match the FBI's hate crime totals, which are included in the response to Question 50, above.

The FBI has worked hard to develop a strategy designed to reduce the number of hate crimes in America. Included in this strategy are efforts to ensure field offices are aware of the communities in their jurisdictions where hate crimes are most prevalent, to provide training and establish liaison with those communities, to aggressively investigate credible hate crime allegations, and to work closely with DOJ attorneys to facilitate successful prosecutions.

Predatory Lending

56. The subprime mortgage crisis is roiling our economy. We need to take significant steps to stop the wave of foreclosures that is sweeping across the nation. We also need to address the unscrupulous and predatory lending practices that contributed to the current situation.

a. What criminal statutes does the FBI use to investigate predatory lending practices by the mortgage industry?

Response:

The FBI investigates mortgage fraud primarily under 18 U.S.C. § 1344 regarding bank fraud, 18 U.S.C. § 1341 regarding mail fraud, and 18 U.S.C. § 1343 regarding wire fraud. Each case is investigated and charged on its own merits, so the charges vary depending on the extent and scope of the fraudulent activity.

b. How many FBI agents are tasked with investigating fraudulent and predatory lending practices?

These responses are current as of 6/22/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00151 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.104

Response:

For the purposes of statistics and analysis regarding resource use, the FBI does not distinguish between mortgage fraud and predatory lending practices. In May 2008, approximately 177 SAs were assigned to mortgage fraud investigations, which constitutes a 50% increase in six months.

c. What FBI unit is responsible for investigating fraudulent and predatory lending practices?

Response:

Fraudulent and predatory lending practices are investigated as white collar crimes by the FBI's field offices. The FBI's Criminal Investigative Division has management responsibility for the mortgage fraud program at the national level.

d. Are criminal penalties a significant part of the Administration's strategy to address predatory lending?

Response:

Criminal penalties are pursued in mortgage fraud investigations subject to prosecutorial constraints, sentencing guidelines, and plea agreements.

e. To what extent is the FBI coordinating with other agencies (such as the FTC, the SEC, and HUD) and banking regulators in pursuing fraudulent and predatory lending? With which banking regulators is the FBI coordinating?

Response:

On the national level, the FBI participates in DOJ's Mortgage Fraud Task Force, the membership of which comes primarily from the Federal law enforcement and regulatory communities. Among others, these members include the IRS' Criminal Investigative Division, the Department of Housing and Urban Development OIG, the Veterans' Administration OIG, the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, and the Postal Inspection Service. On the local level, the FBI has established 36 mortgage fraud

---

Those responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00152 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.105

task forces and working groups whose members include various Federal, state, and local agencies affected by the mortgage crisis.

57. In your written testimony you state that the FBI has more than 1,200 pending investigations into mortgage fraud, and that mortgage fraud investigations have dramatically increased in recent years.

a. Does this total include investigations into predatory lending?

Response:

The FBI is taking a "holistic" approach to investigating mortgage fraud, of which predatory lending is one aspect. If the term "predatory lending" is intended to refer to lenders who intentionally prey on borrowers believed to lack the background or experience to understand that they are agreeing to mortgages they are unlikely to be able to pay over the long term, it appears that this practice may be less prevalent than an inclination by financial institutions to make loans without exercising the "due diligence" to ascertain a potential borrower's true economic status. The FBI's mortgage fraud investigations are designed to identify fraudulent aspects of these mortgage transactions, including possible predation by mortgage lenders.

b. If so, how many of these investigations are investigations into predatory lending, as opposed to investigations into "fraud for profit" or investigations into the defrauding of mortgage lenders?

Response:

In its records regarding mortgage fraud investigations, the FBI does not maintain statistics that distinguish cases founded on predatory lending from those premised on fraudulent borrowing. It does appear, though, that what initially appears to be predatory lending is often instead attributable to the use of relaxed underwriting standards driven by the housing boom of the past several years. The inclination of lenders to underwrite risky mortgages using these relaxed standards is the product of several factors, including the rapid equity growth in residential property and the bundling and quick selling of mortgages, which has mitigated the underwriters' risk.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00153 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.106

58. In January, the FBI reported that it initiated criminal inquiries into 14 corporate players in the sub-prime industry. According to news reports, the Bureau is looking at sub-prime lenders and brokers, as well as the banks that securitized and sold subprime loans. According to the reports, the FBI is looking into possible accounting fraud and insider trading by these companies.

a. Please provide an update on the status of these inquiries.

Response:

Corporate fraud investigations related to the sub-prime lending crisis center on valuation frauds, deceptive financial disclosures, misleading and fraudulent marketing practices, and the illegal profiting by corporate executives from insider information. These investigations, which target lending institutions, brokerage houses, hedge funds, investment banks, and due diligence firms, are complex, white-collar cases that are both resource and time intensive. A limited number of these investigations, such as the indictment of Mario Levis, the Treasurer and Senior Vice President of Doral Financial Corporation, have yielded positive results. Many of these investigations are, though, still pending and will require significant time and personnel resources to complete.

b. Are there plans to expand these inquiries or open new inquiries to cover additional companies?

Response:

The FBI has expanded the number of on-going corporate fraud investigations related to the sub-prime crisis to 17. As the mortgage market and Wall Street firms receive additional scrutiny from regulators and independent accountants, we suspect this number may increase.

c. If there is not enough evidence to support a criminal action against a company, will the FBI be providing the SEC with the results of your inquiries so that the SEC can consider pursuing civil actions?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00154 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.107

Response:

The FBI has worked, and will continue to work, closely with the Securities and Exchange Commission (SEC) as each agency conducts its investigations related to sub-prime mortgages. If the FBI investigates allegations of corporate fraud by a public company, the SEC will be apprized of the investigation and will have the opportunity to pursue any actions it deems appropriate.

d. As a result of these inquiries, are you seeing any patterns or themes that could be addressed legislatively to help prevent a recurrence of the problems in the subprime lending industry?

Response:

The current circumstance appears to be the result of the interaction of multiple factors, including historically low interest rates, rising real estate values, extensive use of leveraging in the derivatives market, an absence of regulatory control (including the lack of control related to the "credit default swap" market), and the increased use of mortgage-backed securities, especially high-yielding securities backed by sub-prime loans. The FBI will be pleased to work with DOJ, OMB, and the Congress to develop legislation in this area.

59. According to news reports, the SEC and several states are also conducting investigations into key corporate players in the subprime mortgage industry. Is the FBI coordinating with the SEC and state investigators?

Response:

The FBI has worked, and will continue to work, closely with the SEC as each agency conducts its investigations. As indicated above, the FBI has expanded the number of on-going corporate fraud investigations related to the sub-prime crisis to 17. Although these investigations are conducted independently and neither agency directs the actions of the other, FBI and SEC investigations are coordinated not only at the local level where the investigations are taking place, but also at the national level through the agencies' headquarters offices in Washington, D.C. The working relationship between the two agencies has yielded positive results, and these coordinated efforts are expected to continue this trend.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00155 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.108

Rule of Law in Iraq

60. The creation and maintenance of a functioning law enforcement and judicial system in Iraq is crucial to the future of Iraq. I would like to know more about the role of the FBI in this effort.

a. Please describe the efforts of the FBI in Iraq, including:

i. The Major Crimes Task Force;

ii. The Legal Attaché; and

iii. Any other FBI involvement with rule of law initiatives.

Response to subparts i, ii, and iii:

The Major Crimes Task Force (MCTF) was formed in response to the kidnapping and murder of several Iraqi public officials that had gone unaddressed by the Government of Iraq. One of those murdered was the third ranking judge in the country. None of these crimes were prosecuted and only a small number led to active police investigations. The pursuit of justice for these crimes was the driving force behind the MCTF's formation. Although the MCTF was initially proposed in early 2005 in concept, it was not formalized until a June 2005 announcement by then AG Alberto Gonzales. In November 2005, the MCTF began the process of selecting and training Iraqi police officers. The MCTF is funded with foreign assistance funds from the Department of State through an Interagency Agreement with DOJ. The mission of the MCTF is to investigate attacks on the stability of the nation and to train a core group of Iraqi National Police Officers in complex criminal investigations. It is a joint U.S.-Iraqi major crime investigative task force comprised of 13 vetted Iraqi police officers from the Ministry of Interior, five Language Specialists, and 10 DOJ investigators, which include 4 FBI Agents and 2 each from the DEA, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the United States Marshals Service. The day-to-day operations of the MCTF are overseen by the Baghdad Deputy Legal Attaché and two Assistant Legal Attachés on one-year assignments to Baghdad. The FBI's Counterterrorism Division provides the FBI agents, who are in Iraq on 90-day temporary duty rotations. An Iraqi investigative judge

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00156 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.109

authorized by the Central Criminal Court of Iraq (CCCI) provides judicial oversight of all MCTF investigations.

This is a capacity-building operation in which U.S. assets serve as senior advisors and mentors to Iraqi task force members. The MCTF currently supports 24 multi-faceted investigations authorized by the CCCI investigative judge. This includes participation in crime scene investigations, analysis of physical evidence, witness and suspect interviews, and related investigative activities.

In addition to the MCTF, the role of the Baghdad Legat in the Law and Order Task Force (LAOTF) has been to coordinate the training of Iraqi police officers. The LAOTF is a DoD effort begun in March 2007 to build an Iraqi criminal justice system in Baghdad for the independent, evidence-based, and transparent investigation of major criminals in preparation for their trials before the CCCI. This task force was modeled after the MCTF, initiated by Multi-National Forces - Iraq and supported by DOJ with the assignment of two senior DOJ trial attorneys, one FBI Agent, one DEA Agent, and two ATF Agents. The LAOTF is positioned to facilitate access to investigative judges, jailed criminals, and the police. While the LAOTF is primarily a U.S.-led and resourced initiative supported by only four Iraqi investigators, the FBI has trained approximately 35 investigators to support LAOTF investigations. The LAOTF initiative is one of the cornerstones of General Petraeus' plan to stabilize Iraq.

In the past, the FBI worked with the Regime Crimes Liaison Office (RCLO) on the investigation and successful prosecution of Saddam Hussein, "Chemical" Ali, and other high ranking members of Saddam's former regime. In October 2007, the FBI stopped staffing the RCLO, as all investigations had been completed. It is our understanding that the RCLO is now comprised only of DOJ attorneys.

b. How many FBI agents are involved with the Major Crimes Task Force?

Response:

Four agents from the FBI's Counterterrorism Division serve on the MCTF, along with three Agents from the Baghdad Legal Attaché Office.

c. Where is the Major Crimes Task Force located? Are there field offices throughout Iraq?

Those responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00157 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.110

Response:

The MCTF is located in the International Zone, apart from the building housing the Legal Attaché Office. There are no field offices elsewhere.

d. What kind of assistance is the FBI providing to the Iraqi government?

Response:

The FBI established the Iraqi-U.S. MCTF to respond to high profile, major crimes with the assistance of seasoned U.S. law enforcement investigators. With the benefit of funding provided by the Department of State, the FBI also provides police training and mentoring as well as assistance in the development of mechanisms to monitor, investigate, and address police abuses.

e. What kind of progress has the FBI made, and how do you measure that progress? Please include information on specific benchmarks, timelines, and/or goals for the Major Crimes Task Force.

Response:

Since its inception, the MCTF has opened 27 investigations, served 80 arrest warrants, made 17 arrests, and obtained 7 convictions (2 of which resulted in death sentences), in addition recovering 193 pieces of Iraqi antiquities.

f. What are the biggest challenges that the FBI is facing in assisting the Iraqi government? How are you addressing these challenges?

Response:

In the wake of the 2007 military surge to implement the Baghdad Security Plan, overall security in Iraq improved significantly and sectarian violence decreased over 90 percent in Baghdad's security districts. Iraq's security does, though, continue to suffer from waves of insurgent attacks, improvised explosive devices, vehicle-borne improvised explosive devices, explosive formed projectiles, indirect fire, kidnappings, and mass murders. Militia still exert significant influence on the security situation in Iraq, as demonstrated by Jaysh al-Mahdi's

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00158 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.111

aggression against the International Zone between in late March and early and April 2008, and assistance to the Iraqi Government is complicated by the continued activity of these armed groups. Because Iran's influence on Iraqi government institutions may be hampering efforts to establish order in Iraq, the Baghdad Legat has initiated a comprehensive assessment of the threat posed by Iranian intelligence efforts. To enhance liaison relationships and the collection of counterintelligence related information, the Baghdad Legat participates in weekly counterintelligence briefings and in a Strategic Counterintelligence Directorate working group. The Baghdad Legat is also working to develop a long-term relationship with the Iraqi National Intelligence Service.

The Baghdad Legat is helping to bring a viable justice system to the new Iraqi government by assisting Iraqi officers in developing the skill sets needed to conduct investigations. This includes the introduction of a biometrics initiative, developed to enhance the ability of Iraqi officers to analyze forensic evidence, serology, DNA, and fingerprints - skills that are extremely limited in the current Iraqi law enforcement system.

Gang Violence and Meth Smuggling

61. Several months ago, I held a roundtable discussion with Chicago-area law enforcement and crime prevention groups to discuss the problem of gang violence. There is an alarming amount of gang activity in the Chicago region, and urgent action is needed to address it. Please provide me with information on the FBI's current efforts to address gang violence in the Chicago area.

Response:

The FBI operates four VGSSTFs in the Chicago metropolitan area. Two of these task forces are located in Chicago itself and are tasked with addressing gang crime within the city of Chicago. The two other Chicago Division VGSSTFs are located in Lisle and Tinley Park and are tasked with addressing gang crime in Chicago's western and southern suburbs, respectively.

Following are some examples of recent anti-gang efforts in the Chicago Division.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00159 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.112

- Following a lengthy investigation in 2002, 58 members and associates of the Latin Kings were indicted for conspiracy to distribute cocaine in Aurora, Illinois. After all subjects were convicted in 2005, the FBI and the Aurora Police Department formed a Cold Case Homicide Initiative to address a backlog of unsolved murders occurring in Aurora since the late 1980s. In June 2007, an Illinois Special State Grand Jury returned indictments charging 31 members of the Aurora Latin Kings with first degree murder for 22 separate murders.

- In 2005, the "Top 20" initiative was introduced in a joint effort by the FBI's Chicago Division, the United States Attorney's Office, the DEA, the ATF, the Chicago Police Department, and various other law enforcement agencies, which meet monthly as part of a "war council" on gangs. The attendees designate the Top 20 gangs in the Chicago area and focus their resources to disrupt and dismantle the designated gangs.

- In 2006, following a lengthy joint investigation by the FBI and the Chicago Police Department, 55 members of New Breed, a splinter group of the Gangster Disciples, were indicted and arrested. Members of New Breed controlled a large public housing project on Chicago's west side and were implicated in multiple murders stemming from their attempts to control the area's drug market.

- In 2006, 21 members of the Black P-Stones were indicted and arrested following a 3-year undercover operation by the FBI and the Chicago Police Department. Like many of the FBI's Chicago gang investigations, this investigation produced evidence and witnesses that helped to clear multiple murder investigations.

62. One of the primary avenues by which methamphetamine comes into Illinois is through international criminal gangs, who smuggle meth up from Mexico.

a. What is the FBI doing specifically to address these international criminal gangs?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00160 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.113

Response:

Methamphetamine is the second greatest drug threat to the Great Lakes region after cocaine. According to National Drug Intelligence Center data, methamphetamine abuse in the Great Lakes OCDETF Region is at a high level, particularly in rural areas of the region, but the number of reported methamphetamine laboratory seizures in the Great Lakes region has recently decreased significantly, from 933 in 2006 to 582 through November 2007. It appears that much of this decrease resulted from a reduction in the number of methamphetamine laboratories, which is likely due to the inability of small-scale laboratory operators to obtain from retail locations the precursor chemicals necessary for methamphetamine production. Other factors contributing to the decline in production include aggressive law enforcement efforts, public awareness, and the rising availability of Mexican "ice" methamphetamine, which is supplied to distribution centers in the region, including Chicago, primarily by Mexican drug trafficking organizations.

The FBI works closely with its partners to address the drug problem in this area, sharing with the DEA and with appropriate state and local law enforcement agencies intelligence related to drug trafficking. As indicated in response to Question 61, above, the FBI operates four VGSSTFs in the Chicago area. These task forces target the most sophisticated and violent criminal enterprises operating in the area, including international criminal organizations, which typically engage in drug trafficking in addition to a host of other illegal activities. In targeting these enterprises, the FBI seeks to identify the organizations' command and control as well as their methods of operation. This investigative process often reveals related criminal activities, including regional and international drug trafficking. When this type of activity is uncovered, the FBI expands its investigation to disrupt and dismantle these vehicles of drug distribution.

In addition, as part of the DOS Merida Initiative, DOS, DHS, and DOJ are looking into negotiating an agreement that would permit the disclosure to foreign governments of information in the control of the National Crime Information Center. Among other things, it is hoped that this will contribute to the success of the Merida Initiative in identifying and disrupting illicit drug trafficking across the border with Mexico.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00161 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.114

b. Is FBI engaged in coordinated efforts with other agencies to combat this smuggling?

Response:

As noted above, the FBI is engaged in coordinated efforts with the DEA and with appropriate state and local law enforcement agencies to combat the smuggling of illegal drugs. These efforts include broad sharing of intelligence and aggressive VGSSTF operations.

c. Are additional resources needed to combat these meth smuggling gangs?

Response:

Since 09/11/01 the FBI has focused the resources dedicated to investigating drug-related criminal enterprises on those involving multiple criminal matters beyond just drug trafficking. The FBI has, however, continued to target domestic drug trafficking organizations, primarily through participation in OCDETF operations and through our 143 VGSSTFs. The FBI will continue to work with the Congress, OMB, and others in DOJ to identify the funding needed to address the Administration's priorities.

Crack Sentencing Disparity

63. There is an enormous disparity between prison sentences for drug trafficking convictions based on crack cocaine and powder cocaine. Major drug traffickers import large quantities of powder cocaine into the U.S. and distribute it mainly to major urban areas. Street dealers sell powder cocaine to addicts or use a simple stove-top cooking process to convert it into crack, which they also sell to addicts. On the street, dealers sell powder and crack interchangeably. The pharmacological and prenatal effects of crack and powder cocaine are identical, but the sentences for crack are 100 times more severe than those for cocaine, and the average crack sentence is 43% longer than the average cocaine powder sentence. To make matters worse, the impact of this disparity most affects minority communities. Crack convictions are the single biggest contributor to the over-representation of African-American men in our federal prisons. Do you support a reduction in the disparity between crack and cocaine powder sentences?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00162 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.115

Response:

Please see the response to Question 42, above.

Criminal Fugitives

65. A recent series of articles in the *St. Louis Post-Dispatch* focused on a long-standing problem in public safety: fugitives who escape arrest by crossing state lines and then victimize more people. In state after state and year after year, fugitives are stopped by the police but then released because the warrant for their arrest was not in a national database of warrants or because the state that issued the warrant refused to pay the costs of transporting that fugitive back to their state for prosecution. In tragic story after tragic story, innocent people are murdered, raped, sexually assaulted or victimized in other ways by fugitives who were caught and released. The *Post-Dispatch* series highlighted the following problems, among others:

• More than a third of felony warrants are not entered into the National Crime Information Center (NCIC) database that is routinely checked by law enforcement officers across the country. This includes warrants for violent felonies like homicides and sexual assaults.

• When fugitives are found in other states, authorities routinely refuse to pick them up because they lack jail space for them or they are unwilling to pay the cost of traveling to that state and transporting the fugitive. This is often the case even for warrants based on violent crimes.

The FBI's NCIC Advisory Policy Board reportedly convened a task force last year to examine this issue.

a. What is the FBI doing to address this problem?

Response:

The FBI's CJIS Division is working with the APB and its Warrant Task Force to increase the number of warrants entered into the National Crime Information Center (NCIC) system. Although participation in, and the entry of records into, the NCIC system are voluntary, law enforcement agencies across the country

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00163 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.116

make extensive use of the system. An average of 167,000 records are entered into NCIC monthly, with the highest concentration being the entry of extraditable felony warrants. While the entry and removal of NCIC records is highly dynamic, at any given time NCIC contains records on approximately 1.4 million subjects. The use of NCIC by law enforcement officials results in the apprehension of approximately one thousand fugitives every day.

b. Has the FBI task force reached any conclusions or made any recommendations? If so, please describe them.

Response:

The task force recommended that information be gathered from Federal, state, and local repositories (or warrant systems) to assess the level of record entry into the national system. The task force's goal was to produce a "score sheet" for state and local agencies that illustrates the extent of their participation in the entry of warrants, with the idea that, if a police chief or sheriff is made aware of a department's poor record entry performance, that department will be moved in the direction of greater participation.

This initiative began as a pilot in three states, but data collection efforts have been frustrated by the absence of local repositories (many states and localities do not have repositories, relying entirely on the national system). Data collection is also inhibited by the reluctance of some local agencies to participate, and the task force recognizes that in some circumstances the entry of a warrant into a national system could impact an ongoing investigation. The next meeting of the task force will address these issues, review results, and discuss other means of collecting necessary information.

c. What can Congress do to assist the FBI's efforts to address this problem?

Response:

As noted in the question, the primary reason an agency refuses to extradite is the lack of funds to support travel to another jurisdiction to retrieve an arrested fugitive. Experience indicates that an effort to make the entry of warrants or extradition mandatory would be resisted by state and local officials and may be an unconstitutional unfunded mandate. The United States Marshals Service (USMS)

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00164 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.117

has advised that DOJ can assist state and local governments in the extradition of out-of jurisdiction fugitives through the use of the Justice Prisoner and Alien Transportation System, which is managed by the USMS. The USMS currently provides extradition assistance to state and local law enforcement agencies through a reimbursable agreement.

Sentinel

66. I understand that the FBI is currently implementing the second phase of Sentinel. An August 2007 audit by the Justice Department's Inspector General highlights Sentinel's successes and commends the FBI for its cooperation in complying with recommendations made in earlier audits, but also identifies scheduling and cost concerns. Phase 1 of the system was completed in 14 months instead of the planned 12 months. The Inspector General attributed the delay to four causes: an unrealistic schedule, Lockheed Martin's delay in fully staffing the project with appropriate personnel, difficulties in integrating commercial off-the-shelf software components to work as a whole system, and difficulties in measuring progress against the approved schedule. What is the FBI doing to ensure that the mistakes made in Phase I are not repeated in future phases of the program?

Response:

In order to ensure the future Sentinel phases progress smoothly and on schedule, the FBI is addressing each of the IG's four concerns, as follows.

1. Unrealistic schedule. The Sentinel PMO reviewed Phase 1 thoroughly and determined that the primary cause of delayed completion was that the overall development and deployment approach used for Phase 1, a "waterfall approach" (where all capabilities are deployed at the end of a phase), was not the optimum approach for a complex project such as this. As a result, the PMO changed to an incremental development methodology, in which capabilities are developed and deployed incrementally throughout the phase.

2. Delayed staffing. Lockheed Martin (LM) has developed a hiring plan based on required task completion and is currently increasing hiring in support of Phase 2 and beyond. LM tracks reports to the PMO monthly regarding staffing and remains in compliance with the staffing plan.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00165 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.118

3. Use of commercial off-the-shelf (COTS) products. The Sentinel integration contractor has implemented a number of changes to reduce the risks of integration in Phases 2 through 4, including the greater use of vendors' technical consulting services personnel to install and configure their products to smooth the introduction of new applications.

4. Measuring progress against the approved schedule. The Sentinel PMO has worked to improve the Earned Value Management (EVM) approach, instituting a new, tighter EVM process, reviewing the accuracy of EV data, and forwarding monthly reports regarding this effort to the OIG.

67. Lockheed Martin delivered Phase I of Sentinel on June 19, 2007, two months behind schedule and at a revised contract amount of $59.7 million (a $2.5 million increase over the original $57.2 million figure). The FBI deferred 57 low-level requirements to Phase 2, leaving Lockheed Martin with a smaller deliverable.

a. In light of the deferred deliverables and overall smaller deliverable from Lockheed Martin, why was there not a decrease in the cost of Phase 1?

b. What will be the effect of deferring these deliverables to a later phase on the cost of Phase 2 and on the overall cost of Sentinel?

Response to subparts a and b:

The Phase 1 budget increase was a function of: 1) the "forward purchase" of Phase 2 COTS products; 2) preliminary Phase 2 and strategic planning costs; 3) the early start of O&M; and 4) product integration and performance concerns that delayed delivery by two months, resulting in increased cost and necessitating additional testing to ensure the corrections were consistent with specifications. As a result of the forward purchase of Phase 2 COTS products in Phase 1, the total cost of Phase 2 was decreased by $3.1 million, negating the Phase 1 price increase.

In response to the OIG recommendation that the PMO negotiate a decrease in the cost of a phase during which requirements are deferred, the FBI established a Requirements Working Group that monitors all requirements down to the increment level to ensure that any changes in requirements are adequately captured and reflected in subsequent increments. The request-for-change process

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00166 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.119

includes a PMO evaluation of any potential cost, schedule, or performance impact, and the FBI's Deputy Director must approve any requirement changes beyond those defined in the System Requirements Specification.

c. How has the FBI responded to the Inspector General's suggestion to reconsider the four-phase approach and renegotiate decreases in the costs of future phases if deliverables are deferred throughout the process?

Response:

In response to the recommendation by DOJ's OIG that the FBI reconsider the four-phased approach, the FBI altered the developmental approach to require incremental deliveries during Phases 2 through 4. This will provide opportunities to deliver functionality more quickly and will increase the ability to track requirement completion and schedule compliance. The incremental approach also further reduces the risk of schedule slippage by authorizing discrete deliveries within the phase, called segments. Requirements will be allocated by segment and have been apportioned throughout Sentinel's development. The FBI has advised the OIG that we will be implementing this revised development approach, which is based on an incremental, service-oriented, capability-centric COTS integration approach designed to minimize the need for temporary and complex interfaces between Sentinel and the Automated Case Support (ACS) system during Phases 2 and 3. The OIG has indicated it is satisfied with the PMO's response and has formally closed the recommendation.

68. Lockheed Martin reported costs exceeding the revised contract amount by $4.4 million, but its earned value management (EVM) data continued to show that it was within budget on the project. In August 2007, Lockheed Martin disclosed to the FBI the reasons for the cost discrepancies and proposed an action plan.

a. What has been the FBI's response?

Response:

The OIG cited the EVM issue and made two corresponding recommendations in its August 2007 report. The PMO's Business Management Team has examined the cost discrepancies and developed an action plan to address them. This plan was implemented through LM's Performance Management Process Directive

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00167 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.120

during the November 2007 Integrated Baseline Review. The FBI has informed the OIG of the actions taken to improve the EVM process and has forwarded monthly reports to the OIG. As a result of this effort, the OIG has advised that it is satisfied with the PMO's response and has formally closed one of the two recommendations. The FBI is awaiting a response from the OIG on the second recommendation.

b. Does the FBI still have reason to be concerned with the quality of Lockheed Martin's EVM data, and therefore the effectiveness of its current data in reliably estimating the costs of Sentinel?

Response:

The new incremental development approach and modified EVM process will enhance our ability to review the contractor's technical performance within each segment, and the adoption of a performance-based EVM will provide additional safeguards to ensure program cost and schedule are maintained. The PMO has a detailed EVM process and subject matter experts in place to provide oversight and guidance for both the PMO team and LM. The reporting process has been tightened to ensure adherence to the cost profile. The PMO also employs an internal auditor who reviews 100 percent of every invoice received from the contractor. In addition to Independent Verification and Validation contractors, who provide continual review of all development and fiscal transactions, the FBI's Finance Division has assigned auditors to review contract documents and invoices and the Information and Technology Branch's Program Oversight Unit and Project Assurance Unit conduct independent assessments at specific milestones, providing monthly reviews and health assessments.

c. Aside from the concerns raised by these audits, what other challenges has the FBI faced in implementing Phase I of Sentinel?

Response:

There are two significant challenges inherent in the development of the interface between Sentinel and the legacy ACS system: 1) the design documentation for the ACS system is out of date and does not contain some of the detail required to build a communications interface; and 2) the ACS system is running older

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00168 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.121

database software applications, and locating cleared personnel with expertise in this software is difficult.

d. How have these challenges informed the timeline, cost estimates, content, or planning for future phases?

Response:

The PMO has applied the lessons learned from this challenge in Phase 2 planning. The original FBI Incremental Development Plan anticipated the delivery of functionality to users in three major software releases. Each of these releases was tied to the end of a phase and involved converting one of the three primary legacy capabilities to Sentinel. This approach required the development of a significant amount of interface code to provide a single interface between the two systems.

At the end of Phase 1, the PMO and the Integration Contractor reviewed the lessons learned and determined that the risks to the program's completion cost and schedule were unacceptable. With senior management concurrence, the PMO and the Integration Contractor revised the planning of the remaining three phases to: 1) implement an incremental development/deployment approach that provides capabilities in six-month time frames; 2) deliver end-to-end functionality by case type at the end of each phase; and 3) simplify the interfaces between the legacy ACS and the Sentinel program.

69. A July 2007 Government Accountability Office audit found that the FBI is utilizing several key best practices, including those for evaluating offers and awarding contracts, which increases the chances of success. However, GAO also found that the FBI has not established performance and product quality standards for Sentinel's management contractors. Although the FBI monitors its contractors on a daily basis, GAO argues that a proactive approach is necessary to maximize contractor performance and ensure Sentinel's success. What is the FBI doing to adopt this standards-based approach? If the FBI will not act on this recommendation, please explain why.

Response:

The FBI does not concur with the Government Accountability Office (GAO) view that the FBI should implement performance standards for Sentinel support contractors relative to the quality and timeliness of products and services because

the majority of the management team's work is task oriented and requires written products. All products provided by the support contractors, such as minutes, white papers, and comments, are reviewed and approved by government supervisors. Support contractors submit reports on work accomplishments to their contractor team leaders, who then provide monthly reports to the Business Management Unit. These reports, along with the invoices reflecting the number of hours billed per contractor, are then provided to Unit/Team leaders for their review and concurrence. Through this process, government officials have the opportunity to concur and/or comment on the work performed and hours expended by each support contractor. The FBI believes this provides adequate government oversight of the support contractors.

The PMO has, however, created a corrective action plan relative to this recommendation, as requested by GAO, advising that the PMO will continue to monitor the work of its support contractors and any products created. The Sentinel PMO has also implemented quarterly meetings with the senior managers for each contractor organization and believes this proactive approach will maximize contractor performance and ensure success.

70. The GAO audit also questioned the reliability of the FBI's schedule and cost estimates. For example, according to the IT program management handbook issued by the FBI, previous schedule and cost estimates do not seem to inform future ones. GAO also notes that current cost estimates do not include all relevant costs, such as government labor and inflationary costs. In light of the previous failure of the Virtual Case File program, what is the FBI doing to address the GAO's concerns and ensure the reliability of its schedule and cost estimates?

Response:

The FBI is addressing cost and schedule estimates by conducting monthly Project Management Reviews (PMRs) and bi-monthly Portfolio Reviews. As part of the PMRs, project costs and schedules are reviewed and validated by senior managers. These PMR presentations become a historical reference point for future cost and schedule estimates. During PMRs, the following items are reviewed and discussed:

- Planned, approved, committed, and obligated funding for the project.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00170 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.123

- Planned versus actual development costs to date.
- Planned versus actual project management office costs to date.
- Schedule milestones, dependency dates, and leading lagging indicators.
- Schedule performance, including planned activities versus actual progress being made against the baselined plan to identify lagging critical path tasks.

Every other month, executive managers conduct Portfolio Reviews to evaluate progress. The same types of information briefed at a PMR are also briefed during a Portfolio Review.

These monitoring controls will enable the FBI to maintain historical cost and schedule information that can be referenced to assess the validity of projected costs for both ongoing and future procurements.

FBI/DHS Fingerprint Database Integration

72. Over a decade has passed since Congress initially urged the integration of the FBI and DHS fingerprint databases, and over fifteen years have passed since the databases were originally conceptualized. What is the current status of the integration effort? When will the two databases be fully interoperable?

Response:

In July 2006, the FBI and DOS were directed to work together to implement the DOS-FBI Ten-print Pilot Program for conducting full IAFIS searches for visa applicants at 12 agreed upon Consulate Offices. This pilot was initially deployed in October 2006, when submissions were successfully processed in IAFIS, with criminal history information being returned to the Consulate Offices. The full success of this pilot was demonstrated by the world-wide roll-out of this program to all Consulate Offices in January 2008. The FBI's IAFIS is currently receiving an average of 30,000 visa applicant submissions per day through DHS's Automated Biometric Identification System (IDENT) system, which includes a subset of extracted IAFIS data.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00171 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.124

With DHS's decision to transition to a ten-print system in 2005, DOJ, DOS, the FBI, and DHS (the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program) agreed to pursue full interoperability between the DHS IDENT system and the FBI's IAFIS, forming a multi-agency Interoperability Integrated Project Team tasked with achieving an automated bi-directional information sharing solution based on biometrics. At that time, the FBI was providing extracts of wanted person and "known or suspected terrorist" data to DHS through an inefficient and partially manual process that did not allow for a reciprocal information exchange.

A biometric-based information sharing pilot known as the interim Data Sharing Model (iDSM) was implemented in September 2006. The iDSM was developed as a short-term interoperability solution allowing for a reciprocal exchange of biometric data subsets between the FBI's IAFIS and DHS's IDENT in near real time. The data included 673,000 fingerprint images for FBI wanted persons from IAFIS, 399,000 Expedited Removals from DHS, and 24,800 DOS Bio Visa Denials from IDENT. The iDSM information sharing initiative has provided participating state and local law enforcement agencies with access to biometric-based information in immigration histories for the first time.

The iDSM pilot agencies include DoD, the U.S. Office of Personnel Management, the Boston Police Department, the Dallas County Sheriff's Office, and the Harris County (Texas) Sheriff's Office. Since the deployment of iDSM in September 2006, there have been more than 417 positive identifications against DHS and DOS immigration data.

In April 2007, DOJ, DHS, and DOS agreed upon a technical architecture for achieving full interoperability, called the Composite Model. The Composite Model includes a Shared Data Component built on the iDSM framework with a separate image repository, through which each agency provides access to "high priority" fingerprint records for the other agencies' searches (similar to iDSM). Initial operating capability (IOC) for the Composite Model will permit NGI searches of IDENT data through the shared services framework, will increase the ability to conduct IDENT searches of NGI data through the shared services framework, will provide an automated response from IDENT for NGI customers, and will provide automated hit notifications to DHS and NGI customers. The IOC will be achieved incrementally. Lessons learned from iDSM, such as the

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00172 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.125

importance of interagency agreements and face-to-face meetings, will be incorporated into the interoperability initiative achieved through the NGI contract. The deployment of NGI will support improved system availability, faster and more accurate identification processing, increased search capacity, and a multi-modal framework. These improvements are expected to occur incrementally from FY 2009 through FY 2012.

In November 2007, DHS began deployment of the ten-print initiative at ten international airports, during which Customs and Border Protection (CBP) "ten-prints" are collected from in-scope travelers and searched against IDENT, including its watch list. Beginning in December 2007, as a pilot for the Shared Services Component of Interoperability, the CBP ten-print transactions that do not result in IDENT hits are forwarded to the FBI's IAFIS for a full search of the Criminal Master File (CMF). The ten-prints are submitted as criminal inquiry searches and are processed as "non-retains" with a required IAFIS response time of 72 hours. Positive identifications are automatically promoted to the IDENT watch list and are reviewed by DHS upon a subsequent encounter with the individual. As of August 2008, IAFIS has processed a little over two million CBP ten-print transactions and has returned over 5,600 positive identifications with previous criminal history records. It is the FBI's understanding that DHS plans to complete its deployment of ten-print collection to all CBP ports of entry by early 2009. Ten-print transactions will continue to be searched against the CMF.

73. Recently, DHS began testing a pilot program at certain airports – including Chicago O'Hare – to better identify whether foreigners are criminals, illegal immigrants, or terrorists. Under the pilot, all ten fingerprints of foreigners are scanned upon entering the country. The ten-fingerprint scan allows DHS to check the identities of visitors against the FBI's fingerprint database, the Integrated Automated Fingerprint Identification System (IAFIS). When will the results of this pilot program be made available to Congress?

Response:

DHS's US-VISIT Program evaluated the U.S. Customs and Border Protection ten-print initial deployment. The FBI's CJIS Division provided statistical data to support the final evaluation report. DHS has offered to provide the 10-Print Initial Deployment Evaluation Report to the Government Accountability Office and to Congress upon request.

These responses are current as of 6/2/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00173 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.126

Next Generation Identification (NGI)

74. Last month, the FBI announced it had awarded Lockheed Martin the contract for the design, development, and deployment of its Next Generation Identification (NGI) System, a $1 billion biometrics database that builds on IAFIS and may eventually include fingerprints, palm prints, iris patterns, face-shape data, and scars to help law enforcement better identify criminals.

a. How will the FBI integrate this database with other existing databases, both within the DOJ and across agencies (e.g., with DHS)?

Response:

The FBI's CJIS Division has ensured that NGI is compatible with the Electronic Biometric Transmission Specification (EBTS), which is the latest upgrade to the FBI fingerprint specification. This specification complies with standards established by ANSI/NIST-ITL 1-2007 [the American National Standards Institute/National Institute of Standards and Technology - Information Technology Laboratory 1-2007] and includes new record types to facilitate data sharing through new biometric modalities. Integrating biometric data in accordance with the ANSI/NIST standard, the FBI EBTS provides a description of all requests and responses associated with electronic fingerprint and other biometric identification services.

The vision for NGI was established with guidance from the user community, including the CJIS APB and the Compact Council. Although the core capabilities were agreed upon at high levels, the FBI wanted to ensure the IAFIS user community had an opportunity to better define the functionality of each of the capabilities. To acquire the appropriate input, the FBI canvassed the IAFIS user community through stakeholder requests (STRQs) to over 193 groups (over 1,000 individuals), including State Identification Bureaus, State Crime Labs, authorized noncriminal justice agencies, and special interest groups such as the NIST and the National Consortium for Justice Information and Statistics. In June 2006, the APB endorsed the collected STRQs, which allowed the FBI to move forward with the development of NGI's functional and system requirements. Specifically, NGI's Enhanced IAFIS Repository capability will provide the repository infrastructure to support information sharing among other Federal, state, and local identification systems. For example, the interoperability with DHS should allow

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00174 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.127

authorized system users to submit biometric transactions through a single interface that transparently and efficiently retrieves information from both systems and reports the updating of relevant data in either system. The benefits of "linked" searches include faster notifications and reduced hardware costs.

b. What is the FBI doing to ensure the privacy of data in the NGI system?

Response:

Privacy protection measures have been built into IAFIS over the past few decades and have been memorialized in the CJIS Division's security policy. As discussed in response to Question 41b, above, an Information System Security Officer is assigned to IAFIS to ensure operational security is maintained on a day-to-day basis, testing roles and rules as part of the security certification and accreditation process. All users are required to affirmatively acknowledge "Rules of Behavior" annually as part of security awareness training, and the E-Government Act of 2002 requires an evaluation of systems that collect personally identifiable information to determine whether information is being appropriately and adequately protected. An NGI Privacy Impact Assessment (PIA), which focuses on the information to be collected, its intended use, and its intended users, was prepared to assess NGI compliance with the Privacy Act and to examine NGI from a general privacy perspective.

To ensure IAFIS security policies are fully implemented and to prevent the misuse of data, all Federal, state, and local IAFIS users are subject to periodic audits conducted by both the state and the CJIS Division Audit Unit, which reports deficiencies to the CJIS APB's Sanction Subcommittee and the Compact Council's Sanctions Committee. Access may be terminated for improper access, use, or dissemination of records obtained from the system of records.

Immigration Name Checks

76. In 2006, I asked you for a statistical breakdown of the delays for different types of immigration applications. You informed me that for 25,975 naturalization applications, a FBI name check had been pending for more than 120 days and for 44,843 naturalization applications, a FBI name check had been pending for more than one year. How many naturalization applications presently have a FBI name check pending:

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00175 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.128

a. for more than 120 days?

Response:

As of 4/8/08, 77,745 USCIS Naturalization Name Check requests have been pending for more than 120 days.

b. for over one year?

Response:

As of 4/7/08, 41,937 USCIS Naturalization Name Check requests have been pending for more than one year.

77. As you know, last summer saw a large increase in naturalization applications. USCIS Director Gonzalez testified in January before the House Immigration Subcommittee that USCIS saw the increase coming and made plans to deal with that increase. What plans did the FBI make to deal with the foreseeable increase in name check applications?

Response:

The FBI has taken several steps to reduce the number of pending USCIS name checks and to position ourselves to address any increases in the USCIS workload. These steps are articulated in our response to Question 15b, above.

78. On February 11, 2008, FBI officials informed Senate Judiciary Committee staff that the FBI has a new plan for name check processing. Please describe this new plan.

Response:

The business plan developed by the FBI to address pending USCIS name checks is aggressive, logical, and achievable. The plan takes into consideration currently pending USCIS name checks, future incoming workloads generated by USCIS programs, levels of available personnel resources (including both current and predicted resources, and both FBI employees and contractors' personnel), project goals, measurable milestones, and business process improvements needed to achieve the stated goals. The plan provides a schedule, with milestones, for eliminating the pending USCIS name checks. Pursuant to this schedule, the oldest pending name checks will be addressed first, progressing to those name

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00176 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.129

check requests submitted most recently. For additional details regarding the plan, please see the response to Question 15b, above.

Questions Posed by Senator Grassley

Bassem Youssef / "Exigent Letters"

83. As you know, the OIG has criticized exigent letters as an improper way to obtain phone records because they contained false statements promising legal process when none was ever intended and unfounded claims of an emergency when none existed. In briefings to Committee staff, the FBI personnel have excused the use of the letters as an unintentional, mistaken use of the wrong form letter. However, according to a letter from Bassem Youssef's attorney dated March 6, 2008 ("Youssef letter"), Mr. Youssef's supervisor formalized the use of so-called "exigent letters" in a November 18, 2003, policy memorandum. The memo from Glenn Rogers to all Communications Analysis Unit (CAU) personnel stated: "Under the authority of the Exigent Circumstances Letter signed by the appropriate CAU Supervisory Special Agent, [the phone company] will provide transactional records. ..." Such a formalized, written policy would seem inconsistent with the notion that exigent letters were merely sent by mistake and more consistent with a scenario where their use was intentional and routine.

a. Is the information I received about this written policy correct?

Response:

It is not the FBI's position that the use of exigent letters was an "unintentional, mistaken use of the wrong form letter," nor has that position ever been briefed to the Committee's staff. There are four problems with Communications Analysis Unit's (CAU) use of so-called "exigent letters": (1) although the letters asserted that there were exigent circumstances, that was not always true; (2) even when there was truly an emergency situation, CAU maintained no records documenting that fact; (3) many of the letters asserted that a Federal grand jury subpoena had been requested, even though, in most circumstances, a grand jury subpoena had not, in fact, been requested and the intent was to provide the carrier with an NSL; and (4) in many cases, although subsequent legal process had been promised to the carrier, no other process (neither a grand jury subpoena nor an NSL) was delivered in a timely fashion (or sometimes, at all).

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00177 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.130

18 U.S.C. § 2702(c)(4) provides that a communication service provider may voluntarily disclose certain non-content records to a governmental entity. Specifically, a provider may disclose a record or other information pertaining to a subscriber or customer, other than the contents of communications, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay. Emergency disclosures pursuant to this authority stand on their own, are separate and entirely distinguishable from NSLs, require no additional legal process, and are entirely lawful.

On 3/1/07, the FBI published policy governing such requests. Under that policy, a request for an emergency disclosure of records must be approved at a level not lower than Assistant Special Agent in Charge (ASAC) in a field office or Section Chief at FBI Headquarters. Absent extraordinary circumstances that must be promptly documented, the request must be made pursuant to a form letter that makes very clear that production of the records is at the carrier's discretion, promises no other legal process, and explains in short form the facts underlying the FBI's belief that an emergency exists. Accordingly, we believe the FBI's new policy deals precisely with the problems identified by the OIG and appropriately balances privacy concerns with investigative needs in cases of dire, life-threatening emergencies.

The memo from Glenn Rogers referenced in your question is part of the facts and circumstances currently under investigation by the OIG. That investigation is expected to explore all of the facts underlying the practice that developed in CAU to obtain telephone records based on so-called "exigent letters." Because that investigation is ongoing, it would inappropriate for the FBI to comment further.

b. Please provide a copy of the November 18, 2003, memorandum (Exhibit 8 to the Inspector General Interview of Bassem Youssef).

Response:

As stated in response to Question 83a, above, this matter is currently under investigation by the OIG. We defer to the OIG regarding the provision of documents related to their pending investigation.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00178 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.131

c. Please describe the legal authority Mr. Rogers had to direct the collection of phone records in this manner.

d. When did the FBI Office of General Counsel (OGC) first review this memorandum?

Response to subparts c and d:

As stated in response to Question 83a, above, this matter is currently under investigation by the OIG, making it inappropriate for the FBI to comment further.

85. According to the Youssef letter, the OGC also provided incorrect advice, misstating the standard for an emergency request under 18 U.S.C. §2702(b)(8). In an April 26, 2005, email from OGC, Youssef was directed to ensure that people in his unit made exigent requests "only when it is clear to you that the requester cannot await an NSL." However, the legal standard is not simply when the requestor "cannot wait." The statute requires "an emergency involving danger of death or serious injury."

a. When did the FBI OGC first advise the CAU and the Counterterrorism Division of the appropriate legal standard for emergency requests? Please provide any and all documentation corroborating the date on which CAU and Counterterrorism officials were advised of the appropriate standard.

b. Why were CAU and Counterterrorism leadership personnel not properly trained in the legal standard for emergency requests much earlier?

Response to subparts a and b:

Please see the response to Question 83a, above.

86. The Youssef letter also states that as late as March 20, 2007, the Assistant Director of the FBI's Counterterrorism Division asserted in an email to top FBI officials that, "First Tier [i.e. direct] contacts of any terrorist operator should be exigent."

a. Please provide a copy of the March 20, 2007, email (Exhibit 19 of the OIG interview with Bassem Youssef).

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00179 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.132

Response:

As stated in response to Question 83a, above, this matter is currently under investigation by the OIG. We defer to the OIG regarding the provision of documents related to their pending investigation.

b. Does the FBI continue to make "exigent" requests (either in writing or informally) based on this incorrect statement of the standard justifying them?

Response:

FBI personnel are now prohibited from using so-called "exigent letters." As discussed in response to Question 83a, above, emergency disclosures may be obtained as permitted by 18 U.S.C. § 2702 in appropriate circumstances. The policy and required procedure for doing so are set forth in Electronic Communications (ECs) dated 3/1/07 and 6/1/07, both of which have previously been provided to this Committee.

c. Please describe the universe of personnel authorized to make exigent requests today.

Response:

Requests made pursuant to 18 U.S.C. § 2702 must be approved by an official no lower than ASAC in the field or Section Chief at FBI Headquarters.

d. Have these FBI personnel been instructed o[n] the appropriate standard for emergency requests under 18 U.S.C. § 2702(b)(8)? If so, when? Was the instruction prior or subsequent to the Assistant Director stating that all "first tier" contacts "should be exigent."

Response:

Through an 8/25/05 EC, FBI personnel have been instructed that the standard for the emergency disclosure of customer records otherwise protected by the Electronic Communications Privacy Act is whether the service provider believes, in good faith, that an emergency involving death or serious physical injury exists. A 4/7/06 EC updated the standard to conform to the USA PATRIOT Improvement and Reauthorization Act. That standard was reiterated in the 3/1/07

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00180 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.133

and 6/1/07 ECs referenced in response to Question 86b, above, and further emphasized in NSL training conducted after March 2007.

e. What does "first tier" contacts mean? Does the FBI designate or distinguish terrorist suspects into various categories and provide a different standard of procedure for each category?

Response:

In the context mentioned, a first-tier contact is a telephone number in direct contact with a known terrorist operative.

Michael German Transcript

87. What punishment did the FBI official who retaliated against FBI whistleblower Michael German receive?

Response:

In October 2006, the FBI's Office of Professional Responsibility (OPR) imposed a 30-day suspension on the FBI official who retaliated against Michael German. On appeal, the FBI's Disciplinary Review Board reduced the 30-day suspension to a letter of censure. Thereafter, the Director's Office overruled the Board, imposing a 14-day suspension.

88. Is the German case the first time that any FBI official has ever been punished for whistleblower retaliation?

Response:

The FBI recognizes the importance of taking appropriate disciplinary action in response to whistleblower retaliation. The Michael German case is not the only occasion on which an FBI official has been punished for such retaliation. For example, in February 2005, the FBI's OPR imposed a 3-day suspension on an ASAC for attempting to reassign a subordinate Agent who had made a protected disclosure. On appeal, the Appellate Unit vacated the 3-day suspension based on an incorrect understanding of DOJ's whistleblower regulation. Thereafter, the FBI's General Counsel forwarded a letter to DOJ advising that the Appellate Unit

had erred in its analysis of the Department's whistleblower regulation and would not make the same mistake in the future.

In September 2006, OPR dismissed a supervisor who engaged in a number of infractions, including retaliation. The retaliation in this case was not whistleblower retaliation.

In January 2007, OPR proposed the dismissal of an SAC for retaliating against a subordinate Agent who had made a protected disclosure. The SAC retired after being served with OPR's proposed termination letter.

In December 2007, OPR issued a letter of censure to an FBI official who advised a subordinate that he would sue her if she followed through on her threat to file what he viewed as baseless allegations against him. As DOJ concluded during its investigation of the matter, OPR found that the subordinate's allegations were, in fact, baseless, but that the supervisor should nevertheless not have threatened suit.

89. Have the terms of the punishment been communicated to other FBI supervisors? If not, then what deterrent effect can the punishment have to prevent others from retaliating against other whistleblowers in the future?

Response:

OPR provides regular and ongoing training to all FBI field office and Headquarters personnel about the disciplinary process, offenses, penalties, and expected standards of conduct. In addition, OPR sends a quarterly e-mail to all employees that includes a discussion of its most recent decisions, which would include the cases noted in response to Question 88, above, including the penalties imposed. Finally, the FBI's Office of the General Counsel and Office of Equal Employment Opportunity Affairs provide mandatory training for all FBI supervisors relating to the Whistleblower Protection Act and accompanying regulations.

Anthrax Investigation

90. I am extremely frustrated with the inability of the FBI to determine the source of leaked information in the anthrax case. The only thing that seems to have happened so far is a reporter has been fined for refusing to name the source of the leak while the officials

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00182 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.135

who leaked sensitive information escape accountability. With the FBI's ability and willingness to obtain other people's phone records, I find it hard to believe that you cannot figure out which FBI officials were talking to reporters about the Anthrax case.

b. My understanding is that the scope and purpose of the OPR investigation focused on the alleged leaking of classified information regarding scientific evidence in the case, and not on the public identification of Stephen Hatfill as a "person of interest." Do you have any reason to believe that is inaccurate?

Response:

The objective of the DOJ OPR leak investigation was to identify who leaked FISA information and who leaked law enforcement sensitive information about the investigation. For further information on this matter, inquiries should be directed to DOJ's OPR.

c. If the OPR investigation did not focus on identifying the FBI personnel who leaked Stephen Hatfil's name, then is it not necessary for someone to make that determination so that the officials may be disciplined appropriately?

Response:

Please see the response to subpart b, above.

d. Has the FBI referred or considered referring that question to the DOJ Inspector General for an independent determination? Why or why not?

Response:

DOJ's OIG is currently investigating the leak to the media of sensitive information regarding the anthrax investigation. For further information on this matter, inquiries should be directed to DOJ's OIG.

e. Have the results of the OPR investigation been communicated to the FBI?

f. If so, what actions have the FBI taken in response to the OPR findings?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00183 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.136

Response to supbarts e and f:

DOJ's OPR conducted two investigations to identify who leaked sensitive information to the media relative to the FBI's anthrax investigation. One investigation was criminal (leaking FISA information) and the other was administrative (leaking law enforcement sensitive information related to the investigation). Both investigations have been closed and are classified Secret. To date, the FBI has not been provided with the result of either investigation.

FBI Access to Draft IG Reports

93. When the FBI reviews draft reports from the Office of Inspector General for classification or sensitivity issues prior [to] the release to the public and Congress:

a. Which components within the FBI participate in the review?

Response:

The FBI's Records Management Division's Classification Units (CUs) conduct the classification reviews of most OIG draft reports. The CUs are Original Classification Authorities (OCAs), reviewing and classifying documents pursuant to EO 12958. If necessary, the CUs consult with subject-matter experts to ensure the content of the OIG draft report is properly classified. There are several other OCAs in the FBI, and classification review is occasionally conducted by an OCA in the FBI division whose programs or procedures are the subject of the report. Review may additionally be conducted by experts in the subject matter of the OIG report who are more familiar with the relationship of the report contents to law enforcement operations and security.

b. Does the FBI public relations office participate in such reviews? If so, please explain for what purpose.

c. Does the FBI Congressional affairs office participate in such reviews? If so, please explain for what purpose.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00184 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.137

Response to subparts b and c:

Before releasing FBI information to the public or to Congress, the entity releasing the information ensures that relevant parties have conducted the appropriate review and, if this has not occurred, the information is referred for such review.

Jane Turner Verdict

94. In last year's questions, I asked whether the FBI was going to discipline the supervisors responsible for the retaliation found by the jury. Your response indicated that the only two officials responsible, SSRA Craig R. Welken and ASAC James H. Burrus, Jr., had since retired. Your response also stated that the third official, James Casey, had no culpability in the retaliation.

a. What is your strategy for changing the FBI's culture of retaliation?

Response:

Director Mueller is committed to protecting employees from retaliation for whistleblowing and to ensuring fairness in the FBI's disciplinary process. To that end, based on recommendations of the Bell/Colwell Commission, the FBI has adopted changes to improve its disciplinary process. Specifically, key changes designed to improve the transparency and fundamental fairness of the appellate process for all FBI employees were recommended by the Commission and implemented by the FBI on 8/19/05. In addition, the Commission recommended that the "de novo" appellate standard be replaced with a "substantial evidence" standard, which is now being used to review matters on appeal. The Director has also recently adopted changes to the appeals process to improve its effectiveness, allowing the FBI's appellate authority to continue to serve as an important check and balance on the entire OPR process.

Although the FBI can never completely eliminate an employee's fear of whistleblower retaliation, factors likely to induce such fear can be reduced or eliminated. The anonymous nature of inspection leadership surveys (which are conducted prior to internal FBI inspections to assess management effectiveness), private interviews with the inspection staff during these inspections, and executive managers who promote the proper environment all help to reduce the fear of whistleblower retaliation. If an employee nonetheless believes retaliation

has occurred, this may be reported to the Inspection Division's Internal Investigations Section (IIS) or to DOJ's OIG or OPR. FBI employees are also frequently reminded through FBI-wide emails and other mechanisms that there is a procedure established under law (5 U.S.C. § 2303) and implemented by regulation (28 C.F.R. Part 27) that provides a formal avenue for an employee to seek corrective action based on a personnel action taken in reprisal for whistleblowing.

b. How does your strategy deter retaliatory behavior when the senior employees responsible typically avoid discipline by retiring?

Response:

As indicated above, Director Mueller is committed to protecting employees from retaliation. To that end, the FBI has put in place numerous processes to address employees' concerns, including regularly reminding employees of the means by which they may address their concerns, the Bureau's zero tolerance of retaliation, and the sanctions to which an employee will be subject for engaging in retaliatory behavior. If an employee who is eligible to retire elects to retire in lieu of serving a proposed disciplinary sanction, for retaliation or any other offense, the employee may retire. In light of the Bureau's zero tolerance for retaliation and the negative impact that a finding of retaliation has on an employee's career, it is not surprising that an employee who is found to have engaged in retaliation may elect to retire.

c. Given the years of procedural hurdles necessary to definitively establish the misconduct, how do you plan to ensure that such conduct is deterred and disciplined before those responsible retire?

Response:

Upon the receipt of an allegation of whistleblower retaliation, DOJ's OIG conducts an immediate investigation. At the conclusion of the investigation, which may be lengthy depending upon the number of witnesses and the complexity of the issues, the OIG prepares a report and refers the matter to the FBI's OPR for adjudication. OPR then renders a decision as expeditiously as possible. As discussed above, if an employee is eligible to retire and elects to do so before the imposition of OPR's penalty, the employee may retire. However, if

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00186 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.139

the employee retires under the cloud of a pending OPR matter that would likely have resulted in the employee's dismissal, the employee will not: (1) qualify for future re-employment with the FBI; (2) be permitted to return to the FBI as a contractor; or (3) be eligible to receive retirement credentials.

d. What changes, in any, has the FBI undertaken to ensure that such an incident is handled appropriately in the future?

Response:

As discussed above, the FBI has instituted a number of changes to eliminate retaliation and to address potential problems in a quick and proactive manner. For example, in consultation with DOJ's OIG, the FBI has taken corrective action, before a final adjudication, based upon allegations that have been determined by the OIG to have validity. Depending upon the circumstances of the individual case, the complainant may be made whole and the retaliator relieved of supervisory duty pending a final decision in the matter.

e. If Welken and Burrus were still employed by the FBI today, what disciplinary actions do you believe would be appropriate?

Response:

OPR did not adjudicate this matter and is not able to speculate on the findings it might have made or the penalties it might have imposed had it adjudicated the matter. The FBI's Offense Table and Penalty Guidelines do, though, specifically address retaliation. If a finding of retaliation is made and aggravating factors are involved, an employee may be subject to dismissal. "Retaliation against whistleblowing or other protected activity" is specifically identified as an aggravating factor that may result in an employee's dismissal.

f. In what way have the actions of the SAC, with respect to Turner's downgrade in performance and subsequent transfer, been examined?

g. How has the SAC been held accountable for his/her role as the ultimate chief decision-maker?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00187 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.140

Response to subparts f and g:

The actions of all those involved in Turner's performance appraisals and loss-of-effectiveness transfer have been reviewed exhaustively. The jury expressly determined in its February 2007 verdict that neither the SAC at the time of the December 1999 transfer nor any other FBI employee retaliated against Turner by transferring her from Minot, North Dakota, to the Division headquarters office in Minneapolis. The jury found retaliation only with respect to Turner's June 1999 "minimally acceptable/unacceptable" interim Performance Summary Assessment (PSA). The PSA, which is an interim assessment as opposed to a formal, annual Performance Appraisal Report, is developed by an employee's rating and reviewing officials. In Turner's case, these officials were Supervisory Senior Resident Agent Craig R. Welken and ASAC James H. Burrus, Jr. An SAC does not participate in the development of the PSA. (While ASAC Burrus was serving as both ASAC and Acting SAC of the Minneapolis Division in June 1999, his involvement in Turner's PSA was in his capacity as ASAC.)

h. Did James Casey's inspection not directly result in the retaliatory recommendation to downgrade Turner's performance, ultimately leading to her transfer?

Response:

A review of SA Turner's performance revealed she was not carrying out her responsibilities in a manner commensurate with her grade level and experience. The inspection of the Minot Resident Agency (MRA), led by James Casey, determined SA Turner's performance deficiencies had negatively impacted the ability of the MRA to perform its mission. As a result, the Inspection recommendations included a recommendation that SA Turner be transferred to an entity that would afford her closer supervision and a re-evaluation of her performance based on the inspection findings.

i. Was Casey's inspection report complete, truthful, and accurate?

Response:

Casey's report accurately reflected the results of file reviews and performance documentation, as well as interviews of colleagues and outside law enforcement agencies.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00188 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.141

j. Has Casey been promoted since his role in the Turner case? Please explain.

Response:

Yes. James Casey was recently promoted to the position of SAC of the FBI's Jacksonville, Florida, Division.

Gag Order "Agreements"

95. I recently learned that the FBI has been using broad gag order agreements in violation of Consolidated Appropriations Act, 2008, Pub. L. No. 110-161 § 719, 121 Stat. 1844, 2024 (Dec. 26, 2007) ("Section 719"). Congress passed Section 719 to ensure that employees are not forced to sign away their right to contact their elected representatives to report waste, fraud, abuse, or mismanagement. The provision states:

> **No funds appropriated in this or any other Act may be used to implement or enforce the agreements in Standard Forms 312 and 4414 of the Government or any other nondisclosure policy, form, or agreement if such policy, form, or agreement does not contain the following provisions:**
>
> > **These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect**

against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive order and listed statutes are incorporated into this agreement and are controlling.

* * *

Such nondisclosure forms shall also make it clear that they do not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

I have been told that all witnesses in the FBI/OIG review of National Security Letters (NSLs) executed a broad non-disclosure agreement not compliant with Section 719 and that this is routine practice in other investigations as well.

a. Is it true that such broad gag-agreements which fail to comply with Section 719 were used in the FBI/OIG review of NSLs?

Response:

During the first interview of an FBI employee represented by an attorney in the OIG/FBI review of NSLs, and when no other non-disclosure form was available for the OIG's use, a broad non-disclosure agreement form was provided by the FBI to the OIG. The OIG continued to use this non-disclosure agreement form until it was learned that it was overly broad, at which time the OIG ceased its use. Since December 2007, the non-disclosure agreement form used in the OIG/FBI NSL review has complied with Section 719.

b. Is it true that such non-compliant agreements are used routinely in other internal inquiries?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00190 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.143

c. Please provide copies of all non-disclosure agreements the FBI has executed to the Committee so that we may independently assess to what extent the FBI is in compliance with Section 719.

Response to subparts b and c:

The FBI requires all employees to execute form FD-291, *FBI Employment Agreement*, in which the employee agrees not to disclose information from FBI files or acquired by virtue of official employment unless authorized to do so. In 2005, this form was revised to include the language specified in section 622 of the Consolidated Appropriations Resolution of 2003, Pub. L. No. 108-7, 117 Stat. 11, 469 (2/20/03), which is identical to the language in section 719, referenced in this question. This form excludes from its general non-disclosure requirements disclosures made pursuant to the FBI Whistleblower Act, 5 U.S.C. § 2303, and its implementing regulations, 28 C.F.R. Part 27. All FBI employees were required to sign the revised FD-291 in 2005, and all new employees are required to sign this form as a condition of employment.

The FBI uses several additional nondisclosure agreements in connection with access to sensitive or classified information. Form FD-857, *Sensitive Information Nondisclosure Agreement*, is used when an individual who is not an FBI employee, such as a Task Force Officer, requires access to sensitive but unclassified investigative information. Form FD-857 was revised in 2005, and contains the same language from the 2003 Appropriations Act as form FD-291, similarly excluding from its nondisclosure requirements disclosures made pursuant to the FBI Whistleblower Act and implementing regulations.

Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*, is executed, following an appropriate security briefing, by those seeking access to classified information. SF 312, which is used by agencies throughout the Executive Branch, also contains language identical to the language quoted in this question but, as a government-wide form, does not specifically reference the FBI Whistleblower Act. Similarly, Form 4414, *Sensitive Compartmented Information Nondisclosure Agreement*, is executed, following an appropriate security briefing, by those seeking access to information protected by a Special Access Program, generally referred to as Sensitive Compartmented Information. Form 4414 is used throughout the Executive Branch. The current version of Form 4414, which replaced a 1997 version, also contains language identical to the language quoted

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00191 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.144

in this question but, as a government-wide form, also does not specifically reference the FBI Whistleblower Act.

The FBI continues to assist DOJ's OIG in its review of the FBI's use of NSLs. This ongoing investigation is led by the OIG, which retains custody of all original paperwork generated in connection with the investigation. When an FBI employee to be interviewed in this investigation is represented by counsel, the attorney is required to sign a nondisclosure agreement, which is retained by the OIG. The FBI does not have copies of any nondisclosure agreements used in this investigation after 12/26/07, the effective date of section 719. The FBI's Inspection Division also uses form IIS-3, *Nondisclosure Agreement*, which is executed by attorneys representing FBI employees who are interviewed in the course of FBI administrative inquiries.

Copies of forms FD-291, FD-857, SF 312, Form 4414 and IIS-3 are attached as Enclosures A, B, C, D, and E, respectively.

d. To the extent that the FBI has executed non-disclosure agreements that fail to comply with Section 719, please explain why such agreements fail to meet the legal requirements and describe what plans, if any, the FBI has to ensure future compliance.

Response:

Form IIS-3, which is executed by counsel representing FBI employees rather than by FBI employees themselves, does not contain the specific language from section 719 referenced in the question. In particular, form IIS-3 does not explicitly permit "disclosures to Congress, or to an authorized official of an executive agency or the Department of Justice, that are essential to reporting a substantial violation of law." Form IIS-3 does, though, explicitly permit disclosures, without prior FBI authorization, to: the FBI Director, the IIS of the FBI's Inspection Division, the FBI's OPR, the AG, DOJ's OIG, and DOJ's OPR. Form IIS-3 also permits disclosures "required by law, court order or subpoena (and then under seal to the extent permitted by law)."

The FBI is reviewing form IIS-3 and will revise the form to bring it into compliance with section 719 if necessary.

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00192 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.145

FBI Translators

96. In 2004, the DOJ/OIG issued a report on the FBI's Foreign Language Program ("FLP"). This report highlights some serious shortcomings of the FLP, including massive backlogs as well as hiring and quality control difficulties. I have also reviewed the DOJ/OIG's follow-up audit of the FLP in 2005. I am interested in an update on the status of the FLP and I would like clarifications on specific points addressed in the both IG reports:

a. The IG's 2004 report made 18 specific recommendations. How has the FBI responded to those recommendations? Are all 18 fully implemented? Please describe in detail any that are not fully implemented and the reason it has not been implemented.

Response:

The FBI's response to the OIG report was accomplished by letter dated 9/30/04. Because that response is classified, we have not provided it in this unclassified submission. We have attached as Enclosure F the OIG's 10/13/06 letter, which states that, based on the FBI's responses, the OIG "consider[s] all recommendations to be closed."

b. Based on the report's 2005 data, the Language Services Section ("LSS") consisted of 1,338 linguists, of which 931 were contract linguists and 407 were full-time language specialists. According to the 2005 report, the number of LS's linguists grew to 1,338. How many linguists, excluding Special Agents and Analysts with foreign language capabilities, are currently employed by the LSS? Does the LSS continue to maintain a roughly 2:1 ratio of contract to full-time linguists? What is the current ratio? Given the constant and growing need for foreign language services, does the LSS's current level of reliance on contract linguists still make sense?

Response:

As of 3/31/08 the FBI employed 497 full-time Language Analysts and 908 contract linguists providing full-time and part-time services and 52 candidates were in processing for Language Analyst positions. The current ratio of contractors to government linguists is approximately 1.82 to 1. Based on the realities of expanding workloads in existing collections and new targets in new languages, the continued reliance on contract support makes sense as an

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00193 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.146

augmentation of certain low-density resources for short- and mid-term assignments. Because the FBI does not foresee a decline in any of the mission-critical languages or traditional collection targets, increasing the permanent cadre of government linguists is essential to our ability to sustain current activities and to address emerging needs.

c. Does the FBI pay Special Agents who use their foreign language skills on the job a supplemental amount? If so, how does that supplemental pay compare to the budget of the FLP?

Response:

Because of legal and funding restrictions, a foreign language supplement is currently paid only to SAs with Spanish-language proficiency who are assigned to the FBI's San Juan Field Office in Puerto Rico. The President's FY 2009 Budget recommends the initiation of an FBI-wide Foreign Language Proficiency Pay Program as a retention and incentive tool. If approved, this initiative would be funded by an initial $8.7 million of an estimated FY 2009 foreign language program budget of $53,403,000 and would offer incentives for the acquisition, use, and maintenance of critical foreign language skills.

d. In June 2002, the LSS created an English Monitoring Facility, a unit of English-only speakers charged with reviewing non-foreign language material, thereby reducing the workload of LSS's linguists. Is the staff of the English Monitoring Facility included in the headcount of linguists? Given that the LSS had such a backlog of unreviewed audio tapes and documents, could the role of the English Monitoring Facility be adequately serviced by case agents and transcription services, allowing the LSS to employ additional foreign language personnel?

Response:

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

e. The 2004 IG report noted that "nearly 24% of ongoing FISA counter-intelligence and counterterrorism intercepts are not being monitored." Additionally, the report found that a significant amount of audio hours were deleted prior to being reviewed, though the 2005 report noted an improvement. Both reports note that though deleted audio can be retrieved from archives, several reasons make it prohibitive. Is there any

---

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00194 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.147

point in recording foreign language audio if it will not be monitored or reviewed? Is the FBI continuing to delete unreviewed audio? If not, on what date did the erroneous deletions end?

Response:

At the time of collection, there is every intention of reviewing the collected audio materials. The demands on the FBI's Foreign Language Program (FLP) fluctuate, though, and priorities are adjusted frequently to meet the greatest need at any given time, focusing first on current collection in support of the highest priority investigations and then on older unaddressed work related to lower-priority investigations. Although these lower-priority materials may not ultimately be reviewed, the collection still has strategic value because it can be reviewed at a later date, if necessary.

Because counterintelligence collection is both voluminous and perishable, and because the systems used to process FISA collection do not have an infinite capacity to store unreviewed FISA collection online, where it is widely available for remote review by linguists located elsewhere, FBI policy permits the deletion of counterintelligence audio 45 days after the intercept. All FISA collection systems have sufficient data storage capacity to maintain this audio online for 90 days, and nearly all can maintain it online for 120 days, after which unreviewed audio may be deleted from online access. The audio continues to be available in media archives for later reference and review if needed.

f. According to the 2004 report, FBI policy requires Al Qaeda FISA audio recordings to be reviewed within 12 hours of interception, and there is an additional expectation that other counterterrorism FISA audio be reviewed within 24 hours of interception. The report noted that in April 2004, only 64% of Al Qaeda FISA audio and 59% of other counterterrorism FISA audio were received by the Language Service Translation Center within their respective time frames. The appendix containing related information in the 2005 report is classified. However, the 2005 report noted that FBI would implement a "triage" type review of material, such that the highest value audio is reviewed with priority. Has this new policy been formally implemented? What are the current percentages of Al Qaeda FISA audio and other counterterrorism FISA audio received within their respective time frames? Is the new triage policy working? What oversight exists at the case agent level to ensure the proper triage and prompt transmission of foreign language recorded audio to the Language Service Translation Center?

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00195 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.148

Response:

Although the 2004 report refers to an "FBI policy" outlining such time frames, the source document for that "policy" was a short e-mail request sent to field office executive management by a former deputy director in the wake of the 9/11/01 attacks. While that request was not implemented as policy, in November 2005 the FBI did articulate the use of investigative priorities as the basis for specified translation time lines.

Because most of the translation services are provided at FBI field offices, the Language Services Translation Center does not receive all audio materials for processing and does not have the technology to track how quickly audio is reviewed. The FBI has, though, implemented a policy addressing the timeliness of translation support to investigations. LSS managers consistently monitor the need for linguist support, ensuring that highest-priority cases are adequately supported and working closely with field office case agents and local FLP supervisory staff to ensure their case work is transmitted to other offices with available linguists when they cannot complete it in a timely manner. When unaddressed work levels indicate that additional linguist resources are required, LSS managers redirect available linguist support from lower-priority matters.

g. The 2004 report notes that the FBI's Washington Field Office, in an effort to integrate advanced technology into the translation process, allowed system maintenance contractors to "reduce the volume of calls that linguists must review by removing certain unintelligible sessions." How are system maintenance contractors qualified to make such a decision? Are they adequately trained to distinguish a predominantly unintelligible session with segments of significant foreign language conversation from a wholly unintelligible session? Do linguists review the sessions marked for removal by system maintenance contractors? Has the modified Translation Quality Control Policy noted in the 2005 report appropriately addressed this issue?

Response:

The referenced unintelligible sessions are limited to sessions containing only so-called "white noise" (that is, sessions in which there is no discernible audio) or consisting only of data transmissions (e.g., facsimile or modem transmissions). System administrators do not apply this process to sessions that contain any

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00196 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.149

detectable conversation. Before implementing an automated process to identify sessions containing only data transmissions or only "white noise," linguists conducted a lengthy review of specific targets, and they periodically perform spot checks of these targets to confirm that no change has occurred with respect to either the target or the collection.

h. The 2004 report recognized that the LSS was too overwhelmed to properly implement the Quality Control Program as required by FBI policy. For example, only 151 quality control reviews were conducted on the 258 linguists with over one year of experience. This represents a less than 60% compliance rate with FBI policy which requires an annual work review of each linguist with more than one year of experience. Are you satisfied with the Quality Control Program, given that 11% of those reviews resulted in unsatisfactory ratings? Though the 2005 report concludes that the FLP implemented changes that addressed the report's concerns, no tests could be completed. Have these statistics improved significantly since 2004? Please explain.

Response:

As indicated in the chart below, the LSS has implemented a complete Quality Control Program and other changes to address the 2005 report. The Quality Control review process has been streamlined and standardized, and compliance tests can now be completed.

Quality Control compliance is measured each quarter (Q), as indicated below.

Period	Reviews				Reviewers		Reporting
	# Satisfactory	# Not Satisfactory	% Satisfactory	# Disputed	# Certified	# Recertified	% of Field Offices
2d Q, FY 2007	630	52	92	10	19	42	100%
3d Q, FY 2007	417	89	82	25	16	42	98%
4th Q, FY 2007	764	90	89	12	13	23	100%
1st Q, FY 2008	596	46	93	15	0	0	98%

i. According to the 2004 IG report, funding for the FLP increased from $21.5 million in FY 2001 to nearly $70 million in FY 2004 (amended to $66 million in the

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00197 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.150

2005 report), representing a significant increase in funding on a per linguist basis. As noted, this increase included $38.5 million in 2004 supplemental appropriations. What was this supplemental funding used for? How do the current funding levels compare?

Response:

The nonrecurring supplemental was used to address critical linguist infrastructure needs, including increasing the number of contract linguists in critical languages, providing these new linguists with necessary technology (core equipment such as computers, internet access, headsets, and basic human language technology tools), and maintaining collection platforms. It also funded build-outs of FBI facilities designated to receive additional linguists and provided resources necessary to linguists, including dictionaries in more than 60 languages, high-level texts on nuclear, explosive, and warfare terminologies, and enhanced or specialized foreign language training in mission-critical languages.

Since 2004, there has been one enhancement of $5 million, which was appropriated in FY 2006.

j. At the time of the 2004 IG report, the LSS was working on the Electronic Surveillance Data Management System ("EDMS"). According to the 2005 report, EDMS will not be fully deployed until FY 2009. What is the current status of EDMS? If EDMS is operable, what is the current backlog of unreviewed material, and the duration of backlog? How will EDMS alleviate the shortcomings of the LSS as reported in the 2004 and 2005 IG reports, with regards to backlogs, unreviewed deleted material, tracking, etc?

Response:

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

These responses are current as of 6/27/08

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00198 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.151

ENCLOSURE A

QUESTION 95C

FORM FD-291

These responses are current as of 6/27/08

FD-291 (Rev. 7-26-05)

FBI EMPLOYMENT AGREEMENT

As consideration for my employment, or my continued employment, by the Federal Bureau of Investigation (FBI), United States Department of Justice, I hereby agree to be governed by and to comply with the following provisions:

(1) Unauthorized disclosure, misuse, or negligent handling of information contained in the files of the FBI or which I may acquire as an employee of the FBI could impair national security, place human life in jeopardy, result in the denial of due process, prevent the FBI from effectively discharging its responsibilities, or violate federal law. I understand that by being granted access to such information, I am accepting a position of special trust and am obligated to protect such information from unauthorized disclosure.

(2) All information acquired by me in connection with my official duties with the FBI and all official material to which I have access remain the property of the United States of America. I will surrender upon demand by the FBI, or upon my separation from the FBI, all materials containing FBI information in my possession.

(3) I will not reveal, by any means, any information or material from or related to FBI files or any other information acquired by virtue of my official employment to any unauthorized recipient without official written authorization by the FBI.

(4) Prior to any disclosure, I will seek a determination whether the information may be disclosed. I agree to be bound by the guidelines governing prepublication review found in the FBI Manual of Administrative Operations and Procedures (MAOP) as those procedures may from time to time be amended. I understand that, in this context, "publication" includes disclosure of information to anyone by any means. I will submit for review the full text of any proposed disclosure addressed by the MAOP or this employment agreement as required by the MAOP at least thirty (30) working days prior to the proposed publication.

(5) I understand that these restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; Section 7211 of Title 5, U.S.C. (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the FBI Whistleblower Protection Act (5 U.S.C. 2303, 28 C.F.R. Part 27) (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling. I further understand, however, that any such information that is disclosed pursuant to applicable federal law continues to be subject to this agreement for all other purposes, and disclosure to the appropriate entities provided by federal law does not constitute public disclosure or declassification, if applicable, of such information.

(6) Violations of this employment agreement may constitute cause for revocation of my security clearance, subject me to criminal sanction, disciplinary action by the FBI, including dismissal, and subject me to personal liability in a civil action at law, including but not limited to injunctive relief, the imposition of a constructive trust, and the disgorging of any profits arising from any unauthorized publication or disclosure. In that regard, I hereby irrevocably assign all rights, title, and interests in any such profits to the United States.

(7) I have read this agreement carefully. Each of the numbered paragraphs of this agreement is severable and if a court should find any of these paragraphs to be unenforceable, I agree that the remaining provisions will continue in full force.

(8) I have read and understand the MAOP prepublication guidelines that are attached.

(9) I accept the above provisions as conditions of my employment or continued employment by the FBI. I agree to comply with these provisions both during my employment in the FBI and following termination of such employment.

_____ _____ (SEAL)
(Printed Name) (Signature)

Witnessed and accepted on behalf of the Director, FBI, on _____, by _____
(Date) (Signature)

Enclosure 67-_____

1-24 PREPUBLICATION REVIEW

(1) REFERENCES. MAOP, Part 1, Section 1-16 (Outside Employment); Section 1-18 (Political Activities); Section 1-27 (Service as an Expert Witness); Section 20-6 (Outside Employment); and Section 20-28.3 (Administration and Requirements of PTAP). See also 28 C.F.R. Section 17.18 (Prepublication Review) and 5 C.F.R. Part 2635 (Standards of Conduct).

(2) DEFINITIONS

(a) For purposes of this section, an "employee" is an individual who has or has had a position of trust with the FBI by virtue of employment, contract, detail, assignment, joint task force, internship, or other agreement, and through this relationship has or had access to FBI information.

(b) For purposes of this section, "information" includes all information acquired from or relating to FBI files or operations, and any other information acquired by virtue of official employment, duties, contract, or status.

(3) BACKGROUND

(a) Every employee occupies a position of special trust and therefore owes a fiduciary duty to the FBI and to the nation to protect the sensitive and often classified information encountered as a result of such position of trust. All information acquired by employees in connection with official FBI duties and all official material to which employees have access are the property of the United States. Employees must surrender upon demand by the FBI, or upon separation from the FBI, all materials containing FBI information that they possess.

(b) Unauthorized disclosure, misuse, or negligent handling of FBI information could impair national security, place human life in jeopardy, result in the denial of due process, obstruct justice, prevent the FBI from effectively discharging its responsibilities, or violate federal law. Therefore, the FBI has established the prepublication review policy described in this section. This policy provides program guidance and establishes requirements regulating individual conduct. Before disclosing FBI information outside of official duty requirements, FBI employees must submit the proposed disclosures to the FBI for review. This prepublication review affords the FBI the opportunity to assess whether the proposed disclosure includes prohibited disclosures (see section (7), below), to advise the submitting employee of any such concerns, and to work with the employee to resolve such concerns. The prepublication review process also enables the FBI to undertake other lawful actions in appropriate cases to protect its mission and operations. This could include, for example, pursuing lawful efforts to prevent a prohibited disclosure, such as seeking an injunction, or to mitigate potential harm from an impending disclosure.

(c) An employee is obligated to comply with prepublication review requirements by virtue of this provision; as well as the FBI Employment Agreement (FD-291), which all employees sign as a condition of employment; by analogous forms such as FD-868 signed by task force members, contractors, etc.; by the Classified Information Nondisclosure Agreement (SF 312),

66825.154

which all employees sign as a condition of being granted access to classified information; and by the Sensitive Compartmented Information (SCI) Nondisclosure Agreement (Form 4414), which employees with access to SCI information sign as a condition of such access.

(4) FBI PREPUBLICATION POLICY

(a) Employees must not disclose FBI information to unauthorized recipients. Prior to any proposed disclosure (outside of official duty requirements) of FBI information, employees must comply with the FBI prepublication review process as described in this section. Employees who fail to comply with the prepublication review process or who make a prohibited disclosure (see section (7) below) are subject to administrative action, clearance revocation, discipline, civil suit, and/or criminal sanction, as appropriate.

(b) It is the employee's obligation to seek guidance from Records Management Division (RMD) on all prepublication review issues not explicitly covered in this section. The employee should resolve any doubts about the legality or propriety of a disclosure or the applicability of these procedures in favor of submitting a proposed disclosure for prepublication review.

(c) Each provision of this section is severable. If a court should determine that any provision is unenforceable, then that provision will be void, but the remainder will continue in full force.

(5) SCOPE

(a) The FBI prepublication review policy applies to any oral, written, or electronic disclosure of FBI information. The FBI prepublication review policy also applies to disclosures of drafts, initial manuscripts, and similar preliminary works to anyone, including attorneys. The only exception to this rule is for disclosures by an employee who is testifying as a defendant in a criminal case in the United States. In that limited situation, the prepublication review policy does not cover disclosures made during testimony or during privileged conversations between the employee and his/her attorney.

(b) By their very nature, completely extemporaneous oral disclosures cannot be reviewed in advance. This does not mean that an employee can disregard the requirements of this section when making oral disclosures. Except in those rare instances where deferring comment would not be practicable due to unusually compelling circumstances beyond the employee's control, employees must defer comment until they can comply with this policy. If an employee reasonably concludes that deferring comment is not practicable, the employee will not be held accountable for failure to comply with this policy. Such an employee may, however, be subject to postdisclosure administrative action, discipline, and/or criminal sanctions, if warranted by the content of the disclosure.

Example: An SAC is participating in a widely attended social event. A congressman

66825.155

asks about a closed investigation centered in his district. The SAC provides a brief overview of the investigation and, while doing so, discloses classified information. Under these circumstances, the SAC will not be sanctioned for violating the prepublication review policy, but (s)he may be sanctioned for disclosing classified information.

(c) Disclosures that clearly have nothing to do with the FBI or its activities, investigations, missions, or operations and that are not otherwise related to any FBI information are not subject to this policy.

Example: A book of children's stories, an article on stamp collecting, a letter to an editor addressing a proposed sewer bond, or an outline of a presentation on the War of 1812 need not be submitted for prepublication review.

(d) Official speeches, writings, and publications made in the performance of official duties are outside the scope of this policy.

(e) Employees who wish to make court appearances or respond to subpoenas in their personal capacities that could require them to divulge FBI information should contact their Chief Division Counsel or the Office of the General Counsel for additional guidance. Disclosure of DOJ/FBI information in federal or state proceedings is subject to the provisions of 28 C.F.R. Part 16, Subpart B.

(f) To the extent that proposed disclosures involve classified information, prepublication review processing will be conducted in conformance with 28 C.F.R. Section 17.18.

(g) Compliance with this policy does not relieve employees from the obligation to comply with the FBI's outside employment rules or the Standards of Ethical Conduct for the Executive Branch, including any applicable limitations on compensation.

(h) The FBI prepublication review process does not encompass a proposed disclosure's factual accuracy or grammar. Similarly, completion of the prepublication review process does not constitute an FBI endorsement of the author or the material disclosed.

(i) This section is intended to be consistent with and does not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the FBI Whistleblower Protection Act (5 U.S.C. 2303, 28 C.F.R. Part 27) (governing disclosures of illegality, mismanagement, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18,

66825.156

United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by the foregoing authorities are incorporated into this policy and are controlling.

(j) Prepublication review is not required for proposed disclosures encompassed by the foregoing authorities. However, any information disclosed pursuant to these authorities continues to be subject to the prepublication policy for any other disclosure.

> **Example:** An FBI employee may make a disclosure of classified FBI information to appropriately cleared personnel of the DOJ OIG pursuant to the FBI Whistleblower Protection Act without prepublication review. The employee may not, however, make an identical disclosure to a reporter without subjecting the disclosure to prepublication review because disclosures to reporters are not protected by those authorities, even if an identical protected disclosure has been made.

(6) PROCEDURES. The following procedures govern the prepublication review process:

(a) Employees must submit the full text of all proposed disclosures of FBI information to RMD at least 30 workdays in advance of the proposed disclosure. Prepublication review submissions must be made in writing even if oral disclosure is contemplated. For disclosures that cannot reasonably be scheduled that far in advance, the employee must submit the material as far in advance as possible. RMD will endeavor to review material in a timely manner, but the FBI prepublication review requirement will not have been satisfied until the review is complete and the employee has been notified. Priority will be given to reviewing materials of temporal significance to a large number of people.

(b) RMD will conduct the prepublication review and will answer questions from employees about the prepublication review process.

(c) RMD will review and process all requests as follows:

1. If RMD concludes that no review is required, it will inform the employee in writing.

2. If RMD concludes that review is required, it will conduct the review.

3. RMD may consult or coordinate with any person who can assist in determining how to proceed with the prepublication review process. This may include seeking help to assess the content or potential impact of the proposed disclosure or to initiate appropriate responses to the proposed disclosure.

> **Example:** RMD may provide a copy of a proposed disclosure to FBI employees with specialized knowledge in order to assess whether the disclosure contains classified information.

RMD may apprise appropriate FBI management officials of impending disclosures that have the potential to harm FBI operations or that may precipitate media or congressional

interest. Text of any proposed disclosure submitted for prepublication review is presumed to be proprietary and shall not be disseminated to any person who does not have an official need to know such information.

Example: An employee submits for review a manuscript that discusses a past FBI/CIA operation that has been the subject of intense congressional review. RMD may seek the assistance of the CIA in reviewing the manuscript. Additionally, RMD may inform OCA of the likely publication so that OCA may be prepared for subsequent congressional or press inquiries.

4. If RMD believes the employee has breached or is attempting to breach this policy, the FBI Employment Agreement or analogous agreements, SF-312, or Form 4414, it will forward a copy of the request, the proposed disclosure, and any other relevant information to the Office of Professional Responsibility (OPR) for appropriate action. RMD will also forward a copy to the Security Division and the Office of the General Counsel (OGC) for appropriate action. RMD will continue to process any related request, unless otherwise directed by OGC, the Security Division, or OPR.

5. If the proposed disclosure includes material that RMD finds cannot be disclosed, it will notify the employee and propose modifications that would be acceptable. RMD will work with the employee and attempt to resolve all concerns.

(d) As a general rule, RMD will respond to a request for prepublication review within 30 workdays of receipt of all required materials. (The day of receipt is not counted for purposes of calculating the 30 workday period, but the day of response is included.) Additional time may be necessary for voluminous or technical submissions. If the review requires additional time, RMD will provide periodic progress reports and will advise the employee of the anticipated completion date.

(e) An employee may appeal an adverse decision to the AD, RMD. The AD will act pursuant to a delegation of authority from the Director. The decision of the AD, RMD, is final, except decisions relating to the deletion of classified information may be appealed to the Deputy Attorney General per 28 C.F.R. Section 17.18.

(7) PROHIBITED DISCLOSURES

Employees shall not disclose the following types of information to unauthorized recipients, except in the performance of official duties or as authorized by RMD:

(a) Information protected from disclosure by the Privacy Act of 1974, as amended;

(b) Information that is classified or the disclosure of which could harm national security;

(c) Information that reveals sensitive law enforcement, intelligence, counterintelligence, or counterterrorism techniques, sources, or methods of the FBI or any other governmental entity;

66825.158

(d) Information that would reveal grand jury material protected from disclosure by Rule 6(e) of the Federal Rules of Criminal Procedure;

(e) Information that would tend to reveal the identity of a confidential source or the identity of a government agency or authority or private institution which furnished information on a confidential basis;

(f) Information that relates to any sensitive operational details or the substantive merits of any ongoing or open investigation or case;

(g) Proprietary information and trade secrets;

(h) Information pertaining to wiretaps or intercepts, electronic communications (including storage mechanisms), or foreign intelligence protected or regulated by Title III (Title 18, United States Code, Sections 2510-2520) or F.I.S.A. (Title 50, United States Code, Sections 1801-1862);

(i) Information pertaining to currency transaction reports regulated or protected by Title 31, United States Code, Section 5313- 5319;

(j) Tax return information regulated or protected by Title 26, United States Code, Section 6103;

(k) Information pertaining to contractor bids or proposals or source-selection information before the award of the procurement contract to which the information relates;

(l) Any other information the disclosure of which is prohibited by law, Executive Order, or regulation; or

(m) Any other information that the FBI would have discretion to withhold from disclosure pursuant to civil discovery obligations, the Freedom of Information Act and Privacy Act, or any other statute, law, or regulation.

(8) EMPLOYEE ACCOUNTABILITY FOR PERMITTED DISCLOSURES

(a) Disclosures will not be prohibited pursuant to this policy solely because they are critical or disparaging of the FBI, the government, or any individual. Any disclosure by a current employee, however, that adversely affects the ability of the employee effectively and efficiently to fulfill his/her official responsibilities or interferes with the FBI's operations may subject the employee to administrative or disciplinary action for the consequences of the disclosure. Examples of disclosures that are not prohibited under this policy but may subject the employee to disciplinary action are the disclosure of private grievances and disclosures that significantly impair discipline or harmony among coworkers, thus having detrimental impacts on close working relationships where personal loyalty or confidence is necessary, impeding the performance of the employee's duties, or interfering with the regular operations of the FBI. An employee will not be prohibited from making such disclosures but may be held accountable for the consequences of the disclosures.

66825.159

Example: An ASAC publishes a scathing attack on the management style of his SAC and thereby loses the trust and confidence of the SAC, disrupts unit cohesion, and prejudices the effectiveness of the office. The ASAC may be disciplined for those consequences even though he sought and obtained RMD review of the material before publication.

(b) FBI employees may ordinarily speak or write about matters unrelated to their employment if they are expressing their personal views. However, when communicating about such matters, an employee should make clear that he/she is stating his/her personal opinion, not the opinion of the FBI and not his/her official opinion as an employee of the FBI. Particular care in this regard should be taken if the employee is identified as an FBI employee.

Example: An employee is involved in and makes public statements regarding a neighborhood campaign to prevent the construction of a national superstore. The employee should not volunteer the information that she is an FBI employee. If the nature of the employee's employment is already known or becomes known, she should affirmatively advise those who know of her employment that she is expressing her personal opinion and not acting on behalf or expressing the opinion of the FBI.

Example: An employee makes public statements regarding substantial premium increases in one of the health plans available to federal employees. Because the employee's federal employment is relevant to his standing in the matter, he may identify himself as a federal employee eligible for the plan (but not as an FBI employee), but he then should affirmatively advise that he is expressing his personal opinion and not acting on behalf or expressing the opinion of any federal agency.

(c) Certain matters of significant public concern are so closely related to the responsibilities and mission of the FBI that there is a substantial likelihood that any comment on such matters by an FBI employee will be perceived as reflecting the employee's official view as an FBI employee or the views of the agency. Therefore, when communicating on matters closely related to the responsibilities, missions, or operations of the FBI, FBI employees should make absolutely clear that they are expressing their personal opinions. Further, certain employees may be precluded from communicating publicly their personal opinions on particular matters. For example, it may be inappropriate for a senior FBI official to express publicly his/her personal view regarding matters within the jurisdiction of the FBI. This is because, as a practical matter, others are likely to perceive the personal views of a senior management employee possessing substantial policy-making authority as indistinguishable from his/her official position as a senior FBI manager.

Example: A support employee in administration (whose only information comes from media reports) makes public statements regarding a local park widely known for drug trafficking. The employee should not volunteer the information that she is an FBI employee. If the nature of the employee's employment is already known or becomes known, she must affirmatively advise those who know of her employment that she is expressing her personal opinion and not acting on behalf or expressing the opinion of the FBI.

Example: The DAD responsible for the FBI's counterdrug programs should not make

66825.160

public her personal belief that marijuana should be legalized. Notwithstanding any disclaimers she might make, as a practical matter the public may still perceive this as reflecting an official FBI position. Moreover, such a statement may interfere with the DAD's effectiveness in exercising her responsibilities, and/or the FBI's working relationships with other law enforcement agencies.

ENCLOSURE B

QUESTION 95C

FORM FD-857

These responses are current as of 6/27/08

FD-857 (Rev. 9-15-05)

SENSITIVE INFORMATION NONDISCLOSURE AGREEMENT

An Agreement between _____
and the Federal Bureau of Investigation (FBI) regarding the following activities:

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to sensitive information from FBI investigations as required to perform my duties. As used in this Agreement, sensitive information is marked or unmarked information, including, but not limited to, oral communications, the disclosure of which may compromise, jeopardize or subvert any investigation. Sensitive information also includes information relating to closed investigations, the disclosure of which might compromise, jeopardize or subvert other law enforcement activities or investigations. I understand and accept that by being granted access to this sensitive information, special confidence and trust shall be placed in me by the FBI.

2. I hereby acknowledge that I have received an indoctrination concerning the nature and protection of sensitive information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of sensitive information may cause irreparable damage to FBI investigations and that I will never divulge sensitive information to anyone unless (a) I have officially verified that the recipient has been properly authorized by the FBI to receive it; or (b) I have been given prior written notice of authorization from the FBI that such disclosure is permitted. I understand that if I am uncertain as to the sensitive nature or status of information, I am required to confirm from an authorized official that the information may de disclosed prior to disclosure of this information.

4. I have been advised that any breach of this Agreement may result in the termination of my relationship with the FBI. In addition, I have been advised that any unauthorized disclosure of information by me may constitute a violation or violations of United States criminal laws, including Title 18, United States Code, or may lead to criminal prosecution for obstruction of lawful government functions. I realize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I understand that all sensitive information to which I have access or may obtain access by signing this agreement is now and will remain the property of, or in the control of the FBI unless otherwise determined by an authorized official or final ruling in a court of law. I agree that I shall return all sensitive materials which have or may come into my possession, or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; or (b) upon the conclusion of my relationship with the FBI, whichever occurs first.

6. I understand that these restrictions are consistent with and do not supersede, conflict with, or otherwise alter my obligations, rights, or liabilities created by Executive Order No. 12958; Section 7211 of Title 5, U.S.C. (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the FBI Whistleblower Protection Act (5 U.S.C. 2303, 28 C.F.R. Part 27) (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling. I further understand, however, that any such information that is disclosed pursuant to applicable federal law continues to be subject to this agreement for all other purposes, and disclosure to the appropriate entities provided by federal law does not constitute public disclosure or declassification, if applicable, of such information.

7. Unless and until I am released in writing by an authorized representative of the FBI, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to the sensitive information and at all times thereafter.

8. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

9. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of sensitive information not consistent with the terms of this Agreement.

10. I have read this Agreement carefully and my questions, if any, have been answered.

Signature _____ Date _____

Organization (if contractor, provide name and address):

The briefing and execution of this Agreement was witnessed by _____
(Type or Print Name)

Signature _____ Date _____

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the Federal criminal laws applicable to the safeguarding of sensitive information have been made available to me; that I have returned all sensitive information in my custody; that I will not communicate or transmit sensitive information to any unauthorized person or organization; that I will promptly report to the FBI any attempt by an unauthorized person to solicit sensitive information, and that I have received a debriefing regarding the security of sensitive information.

Signature _____ Date _____

Name of Witness (Type or Print) _____

Signature of Witness _____ Date _____

ENCLOSURE C

QUESTION 95C

FORM SF 312

These responses are current as of 6/27/08

66825.165

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual — Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable

312-102

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISOO
32 CFR 2003, E.O. 12958

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

ENCLOSURE D

QUESTION 95C

FORM 4414

These responses are current as of 6/27/08

66825.168

SFN _____

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in the process of a classification determination under the standards of Executive Order 12958 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. I have read this Agreement carefully and my question, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12958, as amended, so that I may read them at this time, if I so choose.

FORM **4414** (Replaces Form 4355
2-97 which is obsolete and will not be used)

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the Military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosure of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including section 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation or purpose of evasion.

_____ *Signature* _____ *Date*

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE: _____ *Signature* _____ *Date*

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

_____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____

(Special Access Programs by Initials Only)

_____ SSN (See Notice Below) _____ Printed or Typed Name _____ Organization

BRIEF DATE_____

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

_____
Signature of Individual Briefed

DEBRIEF DATE_____

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefedon the above SCI Special Access Programs(s):

_____
Signature of Individual Debriefed

I certify that the briefing presented by me on the above date was in accordance with relevant SCI procedures.

_____ Signature of Briefing/Debriefing Officer _____ SSN (See Notice Below)

_____ Printed or Typed Name _____ Organization (Name and Address)

NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

ENCLOSURE E

QUESTION 95C

FORM IIS-3

These responses are current as of 6/27/08

66825.171

HS-3 (2005-05-25)

NONDISCLOSURE AGREEMENT

I, _____ , an attorney licensed to practice in the state of
(Name of Attorney)

_____, as consideration for being granted access to certain FBI-related
(State)

information in connection with my legal representation of Federal Bureau of Investigation (FBI) employee,

_____, as to Administrative Inquiry
(Name of Employee)

263-HQ-_____, agree as follows:
(File Number from Notification Form)

I will not disclose orally, in writing, or by any other means, to any party other than the Director, FBI; Internal Investigations Section/Inspection Division, FBI; the Office of Professional Responsibility (OPR), FBI; the Office of the General Counsel, FBI; the United States Attorney General; the Office of the Inspector General, Department of Justice (DOJ); OPR, DOJ; or otherwise as required by law, court order, or subpoena (and then under seal to the extent permitted by law) - **without the prior written authorization of the FBI** - any information or material derived from or relating to FBI files or any other FBI-related information acquired by virtue of my legal representation of this matter.

I may, however, disclose such information to members and employees of my law firm or office pursuant to my legal responsibilities in this matter, but only based upon a need to know and provided that all persons who receive this information first shall be shown a copy of this nondisclosure agreement and, in a written and signed Certificate such as that annexed hereto, state that he or she has read this nondisclosure agreement and agrees to be bound by the terms thereof. I agree to retain such certificates until the conclusion of this matter and shall make such certificates available to the FBI upon request.

I further agree that all documents released by the FBI in this matter remain the property of the FBI and that, upon the conclusion of this matter or at the FBI's earlier request, I will return all such documents and any copies of them to the FBI.

I acknowledge that the unauthorized disclosure of the aforementioned information would violate this agreement, might additionally violate federal law, regulations or policy, and could form the basis for legal action.

_____ (Signature of Attorney)

_____ (Date)

CERTIFICATE

I,_____, acknowledge that I have reviewed the
(Printed Name)
Nondisclosure Agreement between the Federal Bureau of Investigation and _____,
(Name of Primary Attorney)
executed on _____, and agree to be bound by the terms thereof.
(Date of Agreement)

_____ _____
(Signature) (Today's Date)

ENCLOSURE F

QUESTION 96a

10/13/06 LETTER FROM THE OFFICE OF DOJ'S INSPECTOR GENERAL TO FBI DIRECTOR MUELLER

These responses are current as of 6/27/08

U.S. Department of Justice
Office of the Inspector General

Dallas Regional Audit Office
207 South Houston Street, Room 575, Box 4
Dallas, Texas 75202-4724

October 13, 2006

MEMORANDUM FOR ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

FROM: ROBERT J. KAUFMAN
REGIONAL AUDIT MANAGER

SUBJECT: Action Required to Close Audit Report No. 04-25, The FBI's Foreign Language Program – Translation of Counterterrorism and Counterintelligence Foreign Language Program Material

We received and reviewed your latest comments, dated September 5, 2006. Based upon your current and prior comments we consider all recommendations to be closed.

If you have any questions, please contact me at (214) 655-5000.

Attachment

cc: David Evans (copy provided electronically)
Section Chief
Audit, Evaluation, and Analysis Section

Richard P. Theis (copy provided electronically)
Assistant Director
Audit Liaison Group

Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED ON

SEPTEMBER 16, 2009

STATEMENT OF ROBERT S. MUELLER, III
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
BEFORE THE UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

SEPTEMBER 16, 2009

Good morning Chairman Leahy, Senator Sessions, and Members of the Committee. I am pleased to be here today.

As we discussed when I last appeared before your Committee, the Federal Bureau of Investigation (FBI) has undergone a significant evolution in recent years. From developing the intelligence capabilities necessary to address emerging terrorist and criminal threats to building the administrative and technological infrastructure necessary to meet our mission as a national security service, the men and women of the FBI have adapted to our country's ever-changing needs.

Safeguarding our national security remains our primary concern. Indeed, our top three priorities – counterterrorism, counterintelligence, and cyber security – are all related to national security. I will discuss those areas briefly, and then report on what the FBI is doing, and will continue to do, to address the threats posed by criminal enterprises. My focus today on our criminal programs reflects the FBI's belief that our national security depends on stopping crime, as well as on stopping terrorists.

On the counterterrorism front, Al Qaeda continues to present a threat to the Homeland. We work proactively to detect and identify any potential AQ operatives who may have access to the United States. Domestically, through our Joint Terrorism Task Forces, and overseas, through our Legal Attaches and international partners, we share intelligence and conduct operations to fight terrorists. With respect to self-radicalized or home-grown terrorists, we work with impacted communities, our law enforcement partners and other intelligence agencies to identify and disrupt threats.

Regarding counterintelligence, our adversaries continue to target political and military plans, technology, and economic institutions. We have a comprehensive strategy to improve our understanding of the threats and our ability to counter them.

Cyber-based attacks are a growing threat to national security. The FBI has a unique role in this area, as the only agency with the statutory authority, expertise and ability to combine counterterrorism, counterintelligence and criminal resources to counter this threat. We have also established the National Cyber Investigative Joint Task Force, which brings together eighteen of our law enforcement and intelligence community partners in a joint effort to address this challenging problem.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00224 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.177

Now, I turn to our work in the law enforcement realm. In fighting crime, the FBI continues to focus on areas where our involvement will have a substantial and lasting impact and where the FBI has a specific skill or expertise that will contribute to the success of the operation or investigation. Often times we bring our expertise to bear on joint investigations with our partners in federal, state and local law enforcement. We stand shoulder to shoulder to combat these threats, both operationally, and through the sharing of vital intelligence, in a way that was not done in the pre-9/11 world.

Before I outline our criminal programs, I want to emphasize that whether we are addressing threats to our national security or investigating criminal matters, we strive to protect civil liberties and privacy, not just lives and property.

Today I want to highlight priorities in our criminal programs.

White Collar Crime

Public Corruption

Benjamin Franklin was quoted as saying after the 1787 Constitutional Convention that "Keeping government honest and hence our freedoms intact requires eternal vigilance." Because Franklin's words are as true today as they were then, Public Corruption continues to be our number one criminal priority. The FBI recognizes that fighting public corruption is vital to preserving our democracy and to maintaining our credibility overseas. Whether in the back of a squad car, at a border crossing, in a courtroom, or along the halls of Congress, our public officials must carry out their duties in a just and legal manner.

Through our vigilance, we have achieved some notable successes. In the past two years alone, our efforts have helped convict 1600 federal, state and local officials. We have another 3200 public corruption cases pending, of which approximately 2,500 involve corruption of public officials. But more remains to be done. Because the interests at stake are so important and the magnitude of the problem so great, we have deployed approximately 700 agents to fighting corruption around the country.

The Southwest border is a particular focus of our corruption-fighting efforts. Of the 700 agents leading our charge against public corruption, approximately 120 are working along the Southwest border. We coordinate our investigative efforts along the borders with the Department of Homeland Security, Customs and Border Protection Internal Affairs (CBP-IA), as well as with other federal, state, and local law enforcement agencies, through multi-agency task forces. The result is over 400 public corruption cases originating from that region. So far in FY 2009, there have been over 100 arrests, over 130 indictments and over 70 convictions. Stronger cooperation with the governments of Mexico and Central America is an interagency goal of the United States Government.

One particular case highlights the potential national security implications of public corruption along our nation's borders. In that case, an individual gained employment as a

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00225 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.178

Border Inspector for the purpose of trafficking in drugs. Through our collaborative efforts, she is off the streets today. In fact, she will be off the streets for the next 20 years. We cannot permit those willing to forsake their duties and responsibilities for personal gain to be protecting our borders.

In another public corruption investigation with national security implications, twenty-six current and former department of motor vehicle employees were indicted for taking cash bribes in exchange for fake driver's licenses, ID cards, and, frightening, a hazmat license. Those licenses could have ended up anywhere, used by anyone for any purpose.

Another of our recent operations netted corrupt officials from twelve different federal, state and local government agencies, who allegedly used their positions to traffic in drugs. To date, 84 of those subjects have pled guilty to related charges.

As these cases demonstrate, corrupt public officials compromise our democracy and our safety. They also waste our tax dollars.

We are directing our resources all over the country, but we cannot and, fortunately, do not, do it alone. We rely heavily on our partners at all levels of law enforcement. These cooperative and coordinated efforts are yielding results.

Mortgage Fraud

A byproduct of the upheaval in the housing market has been a drastic increase in mortgage fraud cases. In FY 2008, we had about 1600 cases. As of July 31, 2009, we had over 2600 cases pending. Most of these cases have involved losses of over $1 million. To meet this growing challenge, we have redirected investigative resources and assigned approximately 300 Special Agents the task of investigating mortgage fraud. In addition, we direct 15 task forces and 59 working groups that target mortgage fraud.

Mortgage fraud has devastated many American families during the economic downturn and contributed to undermining confidence in the U.S. financial system. The schemes have evolved with the changing economy, targeting vulnerable individuals, victimizing them even as they are about to lose their homes.

Our success in generating new cases is due in large measure to the innovative ways in which we are utilizing data. We employ statistical correlations and other advanced computer technology to identify patterns in the search for companies and persons engaged in activity that is indicative of fraud. In addition, agents analyze data compiled through Suspicious Activity Reports (SARs) filed by financial institutions and through the Department of Housing and Urban Development (HUD) Office of Inspector General (OIG) reports. We have also worked with the mortgage industry to identify trends indicative of mortgage fraud and to educate the public about mortgage fraud. As potential targets are analyzed and flagged, the information is provided to the appropriate FBI field office for further investigation.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00226 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.179

The FBI's efforts in this area focus on fraud perpetrated by industry insiders. It is industry insiders who, in many instances, facilitate mortgage fraud. By focusing on these facilitators we expect to maximize our finite resources.

As is true across our criminal programs, our partnerships with other federal, state and local law enforcement agencies greatly enhance our effectiveness. Building upon our successful task force model, we have established Mortgage Fraud Task Forces across the country. These task forces are concentrated in areas at high risk for mortgage fraud. Partners vary across the country, but typically include Housing and Urban Development Office of Inspector General (HUD-OIG), the U.S. Postal Inspection Service (USPIS), the Internal Revenue Service (IRS), the Financial Crimes Enforcement Network (FinCEN), the Federal Deposit Insurance Corporation, and State and local law enforcement agencies. This multi-agency approach means additional resources for identifying perpetrators of fraud and additional prosecutive options for brining them to justice. The option of pursuing federal or state charges is particularly beneficial in high-volume markets.

In addition to the task forces, the FBI participates in the national Mortgage Fraud Working Group (MFWG), a collaboration of federal agencies, chaired by the Department of Justice (DOJ). The MFWG facilitates information sharing among the member agencies and with private organizations. The Working Group is building upon the FBI's existing intelligence database to identify industry insiders and criminal enterprises involved in systematic mortgage fraud.

In addition to task forces and working groups, the FBI has also participated in coordinated law enforcement sweeps targeting mortgage fraud. Last year, in just over three months, Operation Malicious Mortgage resulted in 144 mortgage fraud cases in more than 50 judicial districts, with over 400 defendants charged with losses totaling approximately $1 billion. The USPIS, the IRS, U.S. Immigration and Customs Enforcement (ICE), and the U.S. Secret Service all took part in this successful operation. Operation Malicious Mortgage followed Operation Continued Action in 2004 and Operation Quick Flip in 2005.

More recently, in April of this year, 24 individuals were charged with several crimes, including racketeering that related to an extensive mortgage fraud scheme based in San Diego involving 220 properties with a cumulative sales price of more than $100 million.

Health Care Fraud

The National Health Care Anti-Fraud Association estimates that each year, three percent of the nation's health care spending—or more than $60 billion—is lost to fraud. When one considers that the federal government accounted for one-third of the $2.2 trillion in health care spending in 2007 and that federal and state governments combined to cover 46 percent of health care costs that year, the government's stake in fighting health care fraud is clear. Moreover, with health care expenditures rising at three times the rate of inflation, it is equally clear that the stakes are rising and that only a concerted law enforcement response will succeed in addressing this problem.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00227 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.180

To this end, the FBI has formed investigative partnerships with other federal agencies, such as the Department of Health and Human Services-Office of the Inspector General (HHS/OIG), the Food and Drug Administration, the DEA, the Defense Criminal Investigative Service, the Office of Personnel Management, the IRS, the Department of Labor (DOL), and various state and local agencies The FBI also works actively with non-governmental organizations, such as the National Health Care Anti-Fraud Association, the Blue Cross and Blue Shield Association, the National Insurance Crime Bureau, and many other agencies, organizations, and professional associations in an effort to expose and investigate fraud within the system.

The interagency cooperation between the Department of Justice, the FBI, and the Department of Health and Human Services is significant. In May of this year, Attorney General Holder and HHS Secretary Sebelius launched the Health Care Fraud Prevention and Enforcement Action Team (HEAT), a team of key leaders from both DOJ and DHHS, that will enhance inter-agency coordination, intelligence sharing and training among investigators, prosecutors, civil fraud attorneys, and program administrators. Sharing real-time intelligence about health care fraud patterns and practices as well as implementing improved technology are top priorities of this team. This effort will enhance the prompt resolution of complex health care fraud cases and support the prevention of fraud and abuse.

HHS,DOJ and FBI are pursuing health care fraud in every region of the country, targeting resources in health care fraud hot spots. The number of pending FBI investigations has shown a steady increase. In FY 2008, FBI-led investigations resulted in over 800 indictments and informations and nearly 700 convictions. So far in FY 2009, the FBI has over 2400 pending cases, approximately 750 indictments and informations, and almost 500 convictions. The DOJ estimates that since the inception of the Health Care Fraud and Abuse Control program (HCFAC) in 1997, the DOJ has recovered more than $14.3 billion lost to fraud through criminal fines and Federal and State civil settlements in health care matters, predominantly stemming from Medicare fraud.

Earlier this month, the American pharmaceutical giant Pfizer, Inc. and its subsidiary Pharmacia & Upjohn Company, Inc. agreed to pay $2.3 billion to resolve criminal and civil claims arising from the illegal promotion of certain pharmaceutical products. This is the largest health care fraud settlement in the history of the DOJ, a settlement that, according to HHS, will return approximately $1 billion to the government. This case highlights the significant role individuals can play in combating fraud, as whistleblower lawsuits triggered the investigation. Six whistleblowers will receive payments totaling more than $102 million from the federal share of the civil recovery.

In late June of this year, our joint health care strike force efforts resulted in charges against 53 individuals accused of various Medicare fraud offenses, including conspiracy to defraud the Medicare program, criminal false claims and violations of the anti-kickback statutes. Strike Force operations in Detroit have identified two primary practice

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00228 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.181

areas – infusion therapy and physical/occupational therapy – in which individuals devised schemes to defraud Medicare.

In late July, working in concert with our partners, we arrested more than 30 suspects in a major Medicare antifraud operation that spanned the country. In New York, Louisiana, Boston, and Houston, more than 200 agents worked on a $16 million fraud that ensnared several physicians.

Corporate Fraud

The FBI has over 100 Agents assigned to over 580 open corporate fraud investigations. We are on pace to significantly increase our production over last year. In FY 2008, we obtained 160 indictments/informations. As of July 31, 2009, we have already obtained over 130 indictments/informations and, more importantly, 140 convictions. Our successful efforts against corporate fraud have netted billions of dollars in restitution.

In late August of this year, former Stanford Financial Group CEO James M. Davis pled guilty to fraud and obstruction charges. Davis admitted that as part of the fraudulent scheme, he and his co-conspirators defrauded investors who purchased approximately $7 billion in certificates of deposit administered by Stanford International Bank Ltd. (SIBL), an offshore bank located on the island of Antigua. Davis and his co-conspirators misused and misappropriated most of those investor assets, including through more than $1.6 billion in undisclosed personal loans to a co-conspirator, while misrepresenting the company's financial condition, its investment strategy and the extent of its regulatory oversight by Antiguan authorities.

In related cases in June of this year, SFG Chairman Robert Allen Stanford, Chief Investment Officer Laura Pendergest-Holt and several other SFG executives were indicted for conspiracy to commit mail, wire and securities fraud; wire fraud; mail fraud; and conspiracy to commit money laundering. In addition, Stanford and Pendergest-Holt were charged with conspiracy to obstruct and obstruction of an SEC investigation.

As with other programs, we rely on partners to contribute their expertise. We work closely with the SEC, Financial Industry Regulatory Authority (FINRA), the IRS, Department of Labor, Federal Energy Regulatory Commission, Commodity Futures Trading Commission (CFTC) and the USPIS to investigate and build corporate fraud cases. In addition, the FBI is a member of the President's Corporate Fraud Task Force, comprised of investigators from the above agencies. The FBI also participates in the Securities and Commodities Fraud Working Group, a national interagency coordinating body established by DOJ to provide a forum for exchanging information and discussing trends in illegal activity, law enforcement issues and techniques. Finally, the FBI has worked with numerous organizations in the private sector to increase public awareness about corporate fraud and to obtain technical assistance regarding accounting and securities issues and background information on subject individuals and companies. This cooperative, multi-agency, public and private sector investigative approach has resulted in highly successful prosecutions.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00229 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.182

Violent Crime

Criminal Gangs

Criminal gangs and other illicit enterprises, operating in the U.S. and throughout the world, are of increasing concern for domestic and international law enforcement and for the intelligence community. Today, gangs appear to be more violent, more organized, and more widespread than ever before. According to the 2009 National Gang Threat Assessment, gangs are responsible for a staggering 80 percent of all crimes in some communities – from drug distribution to theft to homicide. We maximize our resources to combat these crimes by participating in Safe Streets, Gang, Violent Crime, and Major Theft Task Forces. The FBI's Violent Gang Safe Streets Task Forces operate as long-term embedded teams of federal, state, and local law enforcement officers and prosecutors that focus on disrupting the most violent and criminally active gang threats.

Some gangs are entrenching themselves not just in our inner cities but increasingly in our suburbs and rural areas. According to the National Drug Intelligence Center, 58 percent of state and local law enforcement agencies reported that criminal gangs were active in their jurisdictions in 2008, compared with 45 percent of state and local agencies in 2004.

Criminal gangs have developed networks within many of society's institutions, from the military to the prison system, and they engage in a wide range of criminal activities, from alien smuggling to mortgage fraud, from identity theft to extortion. Many of today's gangs actively use the Internet to recruit new members and to communicate with members in other areas of the United States and in foreign countries.

MS-13 continues to expand its influence in the United States. FBI investigations reveal that MS-13 is present in almost every state and continues to grow its membership, now targeting younger recruits than ever before. To counteract this growth, the FBI formed the MS-13 National Gang Task Force, which is based on a central, intelligence driven command structure to coordinate and develop investigations into federal investigations and prosecutions. Task force agents and analysts coordinate investigations with our counterparts in Mexico and Central America. Another anti-gang effort, the Transnational Anti-Gang Task Force (TAG) has already coordinated over 300 investigative leads this year and has coordinated requests for information from the El Salvador Attorney General's Office and the Policia Nacional Civil of El Salvador. TAG will expand to Guatemala and Honduras. The FBI uses the Enterprise Theory of Investigation and sophisticated investigative techniques with the goal of eliminating entire gangs, from street level operators to gang leaders.

Again, our partnerships are critical to combating this threat. In 2005, Congress established the National Gang Intelligence Center (NGIC) to address increases in gang activity and violence. The NGIC is manned by analysts from multiple federal agencies. The databases of each component agency are available to the NGIC, as are other gang-related databases, permitting centralized access to information. In addition, the NGIC provides operational and analytical support for investigations.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00230 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.183

Using these resources, we have identified those gangs that pose the greatest danger to our communities and targeted them with our combined investigative resources and the same federal racketeering statutes and intelligence and investigative techniques that have been used to attack organized crime. Through joint operations and long-standing relationships with our state, local, and international peers, we have had success.

For example, on May 21, 2009, the FBI's Los Angeles Field Office, in conjunction with the Los Angeles Sheriff's Department, DEA, ICE, BATFE, IRS-CID, and other federal, state and local law enforcement agencies, made 88 arrests and executed multiple state search warrants in an effort to dismantle the Varrio Hawaiian Gardens street gang. Of the 88 arrests, 63 arrests were pursuant to five federal indictments naming a total of 147 defendants. With 35 defendants already in custody prior to the takedown, there are now 98 defendants ready to be prosecuted in federal court on RICO violations and federal hate crime violations. This threat-focused, intelligence-driven takedown, involving more than 40 law enforcement agencies and 1,400 officers, was the largest of its kind in U.S. history.

In another example, on June 17, 2009, DOJ announced the indictments of 26 members of a prison gang on 109 felony charges. The indictments were the culmination of Operation North Star, a yearlong effort of the FBI Violent Street Gang Task Force. The investigation targeted members of prison gangs and their surrogates on the outside. Those surrogates, often girlfriends and wives of the prison inmates, given the task of conveying messages of prison gang leaders and facilitating criminal activity. The charges included money laundering, racketeering and supporting a criminal syndicate. Twenty-four of the 26 people indicted are in custody.

Border Violence

We continue to be deeply concerned about the high levels of violence in Northern Mexico. This violence is often connected to international cartel and gang activity. Drug-related violence is not new to the border area, but shifting alliances among criminal cartels poses additional challenges and opportunities for law enforcement. These international cartels are vying for control over lucrative smuggling corridors across the Southwest border, leading to increasingly violent competition between and within these organizations.

Mexican authorities continue their efforts to cut off drug smuggling routes from Mexico to the United States. As I have previously stated, under President Calderon, and with support from the United States, the government of Mexico has made record seizures of drugs, clandestine laboratories, and cash. In addition, Mexican law enforcement agencies have arrested many high-level drug cartel members, who are being extradited to face prosecution in the United States in record numbers.

As a consequence, some of these efforts have contributed to sporadic outbreaks of violent crime. As law enforcement cracks down on these drug trafficking organizations, the traffickers often turn against each other and against government authorities, increasingly resorting to violent crimes, such as murder, extortion, and kidnappings.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00231 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.184

To address the surge in kidnappings, the FBI works closely with Mexican law enforcement officials on a Bilateral Kidnapping Task Force, as well as with other task forces and working groups along the border. To combat drug-related violence, FBI agents work with the DEA, ATF, and DHS and participate on Organized Crime and Drug Enforcement Task Forces and strike forces, which target the most significant drug trafficking organizations in the region. We have also created the Southwest Intelligence Group, which we have housed with the DEA's El Paso Intelligence Center. Our intelligence group serves as a clearinghouse for all intelligence related to Mexico and provides analysis relating to crime along the border.

Crimes Against Children

To combat criminals who prey upon our children, the FBI has also relied heavily upon our partnerships. In June 2003, the FBI, in conjunction with the Department of Justice Child Exploitation and Obscenity Section and the National Center for Missing and Exploited Children (NCMEC), launched the Innocence Lost National Initiative (ILNI).

ILNI addresses the commercial sex trafficking of children within the United States. The victims of these investigations are all U.S. children. The FBI participates in 34 task forces and working groups throughout the U.S., joining with federal, state and local law enforcement agencies and U.S. Attorney's Offices.

The program brings state and federal law enforcement agencies, prosecutors, and social service providers from all around the country to NCMEC for joint training.

As part of its efforts, multiple times a year, the FBI's Crimes Against Children Unit coordinates a national sting operation called Operation Cross Country. ILNI task forces in 29 cities have participated in the operation by targeting venues such as the Internet, truck stops, motels, and the casinos where children are prostituted. Over 600 law enforcement officers from over 95 state, local and federal law enforcement agencies joined together to rescue 119 child victims and apprehend the predators. To date, over 113 defendants have been charged, largely with state and local violations. Every case initiated through the ILNI is reviewed for possible federal violations, and where applicable, those cases are presented to the appropriate United States Attorney's Office for prosecution.

Overall, the ILNI has resulted in over 300 indictments, almost 500 convictions, over 50 criminal enterprises disrupted and approximately 36 successfully dismantled. Since the inception of Innocence Lost, we have recovered 770 children and helped obtain stiff sentences for those responsible, including three life sentences and other sentences ranging from 25-45 years.

Conclusion

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00232 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.185

What I have discussed today represents only a small cross section of the multi-faceted criminal investigations that the men and women of today's FBI are pursuing to keep our nation secure by keeping our streets and neighborhoods safe. We also continue to combat organized criminal enterprises, both national and international; investigate cyber crimes and sophisticated cyber attacks; address an ever increasing foreign intelligence threat; protect and defend civil rights; and focus on violent crime in Indian Country.

While we have invested considerable resources improving the way we transact our operational and administrative business, we also need to commit the time, effort and resources to cultivate our future leaders. One of our priorities this year has been the initiation of the Leadership Development Program (LDP). This program will better prepare our men and women, regardless of position or specialty, for the challenges of leadership within the FBI, and in the wider intelligence and law enforcement communities we serve. The LDP will engage our emerging leaders in a comprehensive leadership development process, tailored to address both individual aspirations, and the demanding leadership challenges faced by the FBI in the 21st Century.

While we continue to upgrade our technology, integrate new business practices, expand our intelligence capabilities, and develop our future leaders, I want to note that the strength of the FBI has always been, and will always be its people. While each and every FBI employee plays a vital role in providing the public the protection they expect, in a way that the Constitution demands, the Special Agent plays a unique role. No matter what his or her assignment, an FBI Special Agent faces extraordinary risks, each and every day. In the past 12 months, the FBI lost three of our own. We lost Special Agent Sam Hicks, a decorated Baltimore police officer who was part of the Pittsburgh Joint Terrorism Task Force; Special Agent Sang Jun, a top-notch cyber agent who served in the El Paso Division, and Special Agent Paul Sorce, a lifelong street agent who worked on the Detroit Violent Crimes Task Force. Each of these Special Agents made the ultimate sacrifice to keep America safe.

I thank you for inviting me here today. I look forward to working with the Committee as we continue to improve the FBI's ability to keep America safe and maintain and develop the capabilities we need to defeat current and future threats. I appreciate your continued support and would be happy to answer any questions you may have.

###

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00233 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.186

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
"SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF ANTI-TERRORISM TOOLS AND INTER-AGENCY COMMUNICATION"

PRESENTED
JANUARY 20, 2010

Robert S. Mueller, III
Director
Federal Bureau of Investigation
before the
Committee on the Judiciary
United States Senate
January 20, 2010

"Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"

I. Introduction

Good morning Chairman Leahy, Senator Sessions, and members of the Committee. I am pleased to be here today.

As you know, we in the FBI have undergone unprecedented transformation in recent years, from developing the intelligence capabilities necessary to address emerging terrorist and criminal threats, to creating the administrative and technological structure to meet our mission as a national security service.

We have worked to become a full partner in the Intelligence Community. With that comes the responsibility to ensure that we consistently collect, analyze, and disseminate intelligence to those who need it, from our Federal partners in the Central Intelligence Agency (CIA), the National Counterterrorism Center (NCTC), the Office of the Director of National Intelligence (ODNI), and the Department of Homeland Security (DHS), among others, to our international, State, local, and tribal counterparts. As I have often said, today we share information by rule, and withhold by exception.

As recent events indicate, terrorists remain determined to strike the United States. We are particularly concerned about individuals who may be radicalized overseas, both those who live in America and those who live overseas and who may one day return to the United States to

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00235 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.188

perpetrate terrorist attacks. We in the FBI, with our partners in the Intelligence Community, must do everything possible to ensure that does not happen. This will require constant vigilance on the FBI's part, and on the part of every member of the IC. It will require the best and highest use of the intelligence we collect, both individually and as a group.

II. The Changing Terrorist Threat

I want to focus first on the changing terrorist threat.

As the Christmas Day attempted bombing illustrates, the threats we face are becoming more diverse and more dangerous with each passing day. We not only face threats from Al Qaeda, but also from self-directed groups not part of Al Qaeda's formal structure which have ties to terrorist organizations through money or training.

We face threats from homegrown terrorists – those who live in the communities they intend to attack, and who are self-radicalizing, self-training, and self-executing. We face threats from those who may attend training camps overseas – individuals who may live here in the United States, and who may be radicalized here or overseas, and those who may live overseas but plan to travel to the United States to perpetrate attacks.

We also face threats from extremists operating in new sanctuaries around the world. While we disabled Al Qaeda's training and financing mechanisms in Afghanistan in the wake of the September 11th attacks, it is clear that Al Qaeda and its offshoots are rebuilding in Pakistan, Yemen, and the Horn of Africa.

At the same time, we cannot discount the lone offender threat here at home – the individual who may take up arms and strike without notice.

We are using intelligence to identify these potential threats. But the question remains: How do we take the strategic intelligence we possess and turn it into tactical intelligence? In other words, once we have identified a potential threat, how do we determine who might take action, and where and when they may do so? And more importantly, how do we prevent them from doing so?

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00236 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.189

In recent years, our capacity for intelligence analysis has improved dramatically. But as the saying goes, trying to glean actionable intelligence from the flood of information we receive is akin to taking a sip of water from a fire hose. As I noted above, the challenge for all members of the IC is to find links between disparate pieces of information – to use the intelligence we possess, individually and collectively – to form a clear picture about the intentions of our adversaries.

III. Recent Counterterrorism Disruptions

As illustrated by recent events, the terrorist threat has not diminished. But through enhanced intelligence, improved technology, and strong partnerships, we have been able to disrupt several terrorist threats and plots this year.

For example, on December 14, 2009, in Georgia, Ehsanul Islam Sadequee was sentenced to 17 years in prison on charges of material support to terrorists. Syed Harris Ahmed was sentenced to 13 years on similar charges. These individuals conducted surveillance of potential targets in Washington, D.C., and pursued terrorist training overseas. They were part of an online network that connected extremists in North America, Europe, and South Asia.

This past October, in Chicago, U.S. citizen David Headley was arrested for planning terrorist attacks against a Danish newspaper and two of its employees. Headley is alleged to have conducted extensive surveillance of targets in Mumbai for more than two years preceding the November 2008 attack there. Headley is also alleged to have attended terrorist training camps in Pakistan. On January 14, 2010, a superseding indictment was filed against Headley relating to his conspiring with others to plan and execute attacks in both Denmark and India.

In October 2009, in Massachusetts, members of the FBI's Joint Terrorism Task Force arrested Tarek Mehanna on charges of conspiracy to provide material support to terrorists. Federal officials charge that Mehanna and other conspirators discussed their desire to participate in violent jihad against America, including a plot to use automatic weapons to open fire on shoppers and emergency responders at shopping malls in Boston.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00237 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.190

In Minnesota, 14 individuals have been charged in recent months as part of an ongoing investigation into the recruitment of persons from U.S. communities to train with or fight on behalf of extremist groups in Somalia. Four defendants have pled guilty and await sentencing. Charges include providing financial support to those who traveled to Somalia to fight on behalf of al Shabaab, attending terrorist training camps operated by al Shabaab, and fighting on behalf of al Shabaab.

In September 2009, Colorado resident Najibullah Zazi was arrested in New York and was charged with conspiracy to use weapons of mass destruction (explosives) in the United States. As alleged in the indictment, Zazi had received detailed bomb-making instructions in Pakistan. Zazi allegedly purchased components of improvised explosive devices, and had traveled to New York City on September 10, 2009, in furtherance of his criminal plans.

Also in September of last year, in Illinois, FBI Special Agents arrested Michael C. Finton on charges of attempted murder of Federal employees and attempted use of a weapon of mass destruction (explosives) in connection with a plot to detonate a vehicle bomb at a Federal building in Springfield. In his efforts to carry out the plot, Finton communicated with undercover FBI agents and confidential sources that continuously monitored his activities up to the time of his arrest. According to the complaint, Finton also drove a vehicle containing inactive explosives to the Federal courthouse in Springfield and attempted to detonate them.

That same month, in Texas, Hosam Smadi was charged with attempting to use a weapon of mass destruction. Smadi, who was under continuous surveillance by the FBI, was arrested after he placed an inert car bomb near a 60-story office tower in downtown Dallas. As alleged in the indictment, Smadi, a Jordanian citizen in the United States illegally, has repeatedly espoused his desire to commit violent jihad and had been the focus of an undercover FBI investigation.

This past July, in North Carolina, FBI agents arrested an alleged group of homegrown terrorists who were heavily armed and making plans to wage jihad overseas. The seven men arrested – including a father and his two sons – were charged with providing material support to terrorists and conspiring to murder, kidnap, and injure people overseas. The father, Daniel

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00238 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.191

Patrick Boyd, once fought in Afghanistan, and allegedly trained in terrorist camps in Pakistan and Afghanistan. All of the defendants but one are U.S. citizens.

And last May, in New York, four individuals were arrested on charges of conspiracy to use weapons of mass destruction in the United States and conspiracy to acquire and use anti-aircraft missiles. The group allegedly plotted to blow up a Jewish synagogue in the Bronx and to shoot down military planes at the New York Air National Guard Base. As alleged in the indictment, they obtained what they believed to be three improvised explosive devices and a Stinger surface-to-air guided missile from a source who was in fact an FBI informant.

This is merely a sampling of the investigations we have handled over the past year. In each investigation, the resources and the investigative experience of our Federal, State, and local law enforcement and intelligence counterparts proved invaluable. Indeed, we in the FBI could not do our jobs without their critical assistance and their expertise.

IV. December 25, 2009 Attack

On January 6, 2010, Umar Farouk Abdulmutallab, a 23-year-old Nigerian national, was charged in a six-count criminal indictment for his alleged role in the attempted Christmas day bombing of Northwest Airlines flight 253 from Amsterdam, the Netherlands, to Detroit.

Abdulmutallab has been charged with attempted use of a weapon of mass destruction, attempted murder within the special aircraft jurisdiction of the United States, willful attempt to destroy an aircraft, willfully placing a destructive device on an aircraft, use of a firearm or destructive device during and in relation to a crime of violence, and possession of a firearm or destructive device in furtherance of a crime of violence.

According to the indictment, Northwest Airlines flight 253 carried 279 passengers and 11 crew members. Abdulmutallab allegedly boarded Northwest Airlines flight 253 in Amsterdam on December 24, 2009, carrying a concealed bomb. The bomb components included Pentaerythritol (also known as PETN, a high explosive) and Triacetone Triperoxide (also known as TATP, a high explosive), and other ingredients.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00239 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.192

The bomb was concealed in the defendant's underclothing and was designed to allow him to detonate it at a time of his choosing, thereby causing an explosion aboard flight 253, according to the indictment. Shortly prior to landing at Detroit Metropolitan Airport, on December 25, 2009, Abdulmutallab allegedly detonated the bomb, causing a fire on board the plane.

According to an affidavit filed in support of the criminal complaint, Abdulmutallab was subdued and restrained by passengers and the flight crew after allegedly detonating the bomb. The airplane landed shortly thereafter, whereupon U.S. Customs and Border Protection officers took him into custody.

The FBI is responsible for investigating this incident. FBI Special Agents interviewed Abdulmutallab following the attack, and have shared all relevant information with our partners in the IC. We will continue to investigate Abdulmutallab and all individuals connected to him, and we will continue to share all relevant information with our law enforcement and intelligence counterparts. However, because this is an ongoing investigation, we cannot divulge many details at this juncture.

V. Terrorist Watchlisting Procedures

I would like to turn for a moment to terrorist watchlisting procedures and the Terrorist Screening Center ("TSC")

The TSC is a multi-agency center that connects the law enforcement communities with the IC by consolidating information about known and suspected terrorists into a single Terrorist Watchlist. The TSC facilitates terrorist screening operations, helps coordinate the law enforcement responses to terrorist encounters developed during the screening process, and captures intelligence information resulting from screening.

The TSC integrates the law enforcement and intelligence communities by consolidating terrorist information. The current terrorist watchlisting and screening enterprise is a collaborative effort between the TSC, the FBI, DHS, the Department of State, the Department of Defense, the NCTC, and other members of the IC.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00240 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.193

VI. Today's FBI

A. Restructuring of FBI Intelligence Program

To meet our national security mission, we have expanded our counterterrorism operations and honed our intelligence capabilities. We stood up the National Security Branch and the Weapons of Mass Destruction Directorate. We integrated our intelligence program with other agencies under the Director of National Intelligence, with appropriate protections for privacy and civil liberties. We hired hundreds of intelligence analysts, linguists, and surveillance specialists. And we created Field Intelligence Groups in each of our 56 field offices. In short, we improved our national security capabilities across the board.

But we also recognize that we must continue to move forward, to refine programs and policies already in place, and to make necessary changes to our intelligence program.

To that end, we established a Strategic Execution Team, or SET, to help us assess our intelligence program, and to standardize it throughout the Bureau. The SET, made up of agents and analysts, developed a series of recommendations for accelerating the integration of our intelligence and investigative work.

The SET improvements ensure that we capitalize on our intelligence collection capabilities and develop a national collection plan to fill gaps in our knowledge base. Our objective is to defeat national security and criminal threats by operating as a single intelligence-led operation, with no dividing line between our criminal and counterterrorism programs. In short, we want to make sure that nothing falls through the cracks.

To this end, we have restructured the Field Intelligence Groups, or FIGs, in every field office across the country. FIGs are designed to function as the hub of the FBI's intelligence program. They ensure that each field office is able to identify, assess, and attack emerging threats before they flourish.

Following the SET's recommendations, the FIGs now conform to one model, based on best practices from the field, and adapted to the size and complexity of each office. Each FIG

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00241 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.194

has well-defined requirements for intelligence gathering, analysis, use, and production. And managers are accountable for ensuring that intelligence production is of high quality and relevant not only to their own communities, but to the larger intelligence and law enforcement communities.

As a result of these changes, the FIGs can better coordinate with each other and with Headquarters. They can better coordinate with law enforcement and intelligence partners, and the communities they serve. With this integrated model, we can turn information and intelligence into knowledge and action, from coast to coast.

These changes are part and parcel of our ongoing campaign to "Know Our Domain," as we say. Domain awareness is a 360-degree understanding of all national security and criminal threats in any given city, community, or region. It is the aggregation of intelligence, to include what we already know and what we need to know, and the development of collection plans to find the best means to answer the unknowns. With this knowledge, we can identify emerging threats, allocate resources effectively, and identify new opportunities for intelligence collection and criminal prosecution.

We have implemented SET concepts at FBI Headquarters, to improve strategic alignment between the operational divisions and the Directorate of Intelligence. We want to better manage national collection requirements and plans, and ensure that intelligence from our Field Offices is integrated and shared with those who need it at FBI Headquarters and in the larger Intelligence Community.

We will continue to refine not only the manner in which we collect and share information, but the manner in which we analyze that information, to find links between people, cases, and countries.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00242 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.195

B. Improvements to FBI Technology

We have also made a number of improvements to the FBI's information technology systems. We cannot gather the intelligence we need, analyze that intelligence, or share it with our law enforcement or intelligence partners, without the right technology.

As you know, we continue to implement Sentinel, our web-based case management system, which makes it faster and easier to access and connect information from office to office, from case to case, and from program to program.

We are also strengthening the IT programs that allow us to communicate and share with our partners. For example, we are consolidating the FBI's Unclassified Network with Law Enforcement Online, or LEO, which is the unclassified secure network we use to share information with registered law enforcement partners. This will provide a single platform that allows FBI employees to communicate and share with their internal and external partners. Currently, LEO provides a secure communications link to all levels of law enforcement and is available to more than 18,000 law enforcement agencies.

As part of the LEO platform, the FBI is delivering the eGuardian system – an unclassified counterterrorism tool available to our Federal, State, local, and tribal law enforcement partners through the FBI's secure LEO internet portal. eGuardian makes threat and suspicious activity information immediately available to all authorized users. The eGuardian system will work in tandem with Guardian, enabling law enforcement personnel to receive the most current information. In return, any potential terrorist threat or suspicious activity information provided by law enforcement will be made available in Guardian entries and pushed outward to the FBI task forces.

We are also in the midst of developing what we call "Next Generation Identification" system, which expands the FBI's fingerprint-based identification, known as IAFIS, to include additional biometric data. This will better enable us to find criminals and terrorists who are using the latest technology to shield their identities and activities.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00243 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.196

We are also working to improve our confidential human source management system. Intelligence provided by confidential human sources is fundamental to the FBI mission. To better manage that data, we have implemented a program known as DELTA. DELTA will provide FBI agents and intelligence analysts a uniform means of handling the administrative aspect of maintaining human sources. It will also enable FBI Headquarters and Field Offices to better understand, connect, operate, and protect confidential human sources.

Finally, we are improving our crisis management systems. The Operational Response and Investigative Online Network (ORION) is the FBI's next-generation Crisis Information Management System. ORION provides crisis management services to Federal, State, local, and tribal law enforcement and/or emergency personnel. It standardizes crisis and event management processes, enhances situational awareness, and supports the exchange of information with other command posts.

The ORION application is accessible from almost any desktop with FBINET or UNET connectivity using a standard web browser, or by other secure connections providing access to Federal, State and local law enforcement partners It has been used at both the Democratic and Republican national conventions, major sporting events, to include the Olympics, and last year's Presidential Inauguration.

These improvements are necessary for the work ahead of us, and we will continue to develop and implement the necessary tools to combat today's diverse, dangerous, and global threats together with our partners in the law enforcement and intelligence communities.

VII. Conclusion

Over the past 100 years, the FBI has earned a reputation for protecting America that remains unmatched. Many of our accomplishments over the past eight years are in part due to your efforts and your support, and much of our success in the years to come will be due to your continuing support. From protecting the American people from terrorist attack to addressing the growing gang problem to creating additional Legal Attaché offices around the world, you have supported our mission and our budget requests.

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00244 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.197

Mr. Chairman, I would like to conclude by thanking you and this Committee for your service and your support. On behalf of the men and women of the FBI, I look forward to working with you in the years to come. I would be happy to answer any questions you may have.

# # #

VerDate Nov 24 2008 09:56 Jul 07, 2011 Jkt 066825 PO 00000 Frm 00245 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\66825.TXT SJUD1 PsN: CMORC

66825.198