

**OVERSIGHT OF THE FEDERAL BUREAU OF
INVESTIGATION**

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

DECEMBER 14, 2011

Serial No. J-112-57

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

74-263 PDF

WASHINGTON : 2012

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

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

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

KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa	3
prepared statement	70
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	80

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, Schumer, Franken, Grassley, Kyl, Sessions and Coburn	35
---	----

SUBMISSIONS FOR THE RECORD

Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa:	
Eric H. Holder and Robert S. Mueller, III, August 31, 2011, letter	74
Eric H. Holder, October 5, 2011, letter	76
Eric H. Holder, November 14, 2011, letter	77
Mueller, Robert S., III., Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC, statement	82
Weich, Ronald, Assistant Attorney General, Department of Justice, Washington, DC:	
Senator Grassley, August 8, 2011, letter	93
Senator Grassley, September 23, 2011, letter	94
Senator Grassley, November 30, 2011, letter	97

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

WEDNESDAY, DECEMBER 14, 2011

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

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

Present: Senators Leahy, Kohl, Feinstein, Whitehouse, Klobuchar, Franken, Coons, Blumenthal, Grassley, and Sessions.

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

Chairman LEAHY. You can tell, Director, this is an important hearing because you have the A Team of photographers here. You have all the absolute best on the Hill. There used to be one other very good photographer here on the Hill, but he left to go to work for the President. But I do get to see him now and then.

Today the Judiciary Committee will hear from Director Robert Mueller of the Federal Bureau of Investigation. I want to thank the Director once again for agreeing to put his life on hold when called upon by the President earlier this year to continue to serve for another 2 years as FBI Director. His commitment and dedication to service are exemplary, and as I said the last time when I mentioned this, I also want to thank Mrs. Mueller. She is a wonderful person, and I know that she also is willing to put a lot of her life on hold for that. So I hope you will pass on my compliments to her.

Mr. MUELLER. I will, Mr. Chairman, and thank you for that.

Chairman LEAHY. Now, the Bureau plays an integral role in protecting our Nation's security through its counterterrorism investigations and intelligence gathering. Its work has contributed to more than 400 convictions in terrorism cases since September 11, 2011. Knowing this, I remain deeply concerned about a provision of the national defense authorization bill that would mandate—and I stress the word “mandate”—as the Chair of the Senate Intelligence Committee knows, the military detention of certain terrorism suspects, even if they are arrested on U.S. soil.

Director Mueller has written that this provision would adversely impact the Bureau's ability to conduct counterterrorism investigations and inject “a substantial element of uncertainty” into its operations. I appreciate what Director Mueller meant when he wrote that the misguided provision fails to take into account “the reality

of a counterterrorism investigation,” especially the successful convictions that we have gotten in our Federal courts.

Now, Congress needs to do more to support important law enforcement efforts. We should give law enforcement the appropriate tools to combat the growing threat of cyber crime, something Senator Coons mentioned in the other room. More and more, American consumers and businesses are being targeted by sophisticated cyber attacks designed to steal their most sensitive information.

I met with the CEO of one of our largest companies the other day, and he told me all the steps they have taken, the millions of dollars they have to spend, just to defend against cyber attacks, a lot of it coming from foreign countries, competitors, and elsewhere.

In September, this Committee again voted for the Personal Data Privacy and Security Act. It is long overdue legislation that will provide tools to help law enforcement combat cyber crime. And the Senate and the House should promptly pass this measure.

In the last Congress, we made great strides toward more effective fraud prevention. I worked hard with Senators on both sides of the aisle to craft and pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade. We enacted important anti-fraud provisions as well, as part of both health care and Wall Street reform legislation. And I am pleased to see that the FBI has greatly increased the number of agents investigating fraud, leading to more fraud arrests and greater fraud recoveries.

This year, I introduced the Fighting Fraud to Protect Taxpayers Act, which redirects a portion of the fines and penalties collected from wrongdoers back into fraud enforcement efforts. And the bill would lead to substantial recoveries, paying for itself many times over. This Committee voted for the bill more than 6 months ago. It is time for the Senate and the House to pass this bill without further delay to give law enforcement the resources and tools they need to crack down on fraud. We will say we are opposed to fraud, but we have got to give law enforcement the tools to fight it.

I commend the FBI for maintaining its historic focus on combating corruption. I have worked to develop bipartisan, bicameral anti-corruption legislation, the Public Corruption Prosecution Improvements Act. I have also worked on the Civilian Extraterritorial Jurisdiction Act, which would hold accountable American contractors and employees abroad who engage in corruption and contracting fraud, especially when it hurts taxpayers in this country.

At a time when anger at corporate wrongdoing, greed, and corruption is at an all-time high—and I might say anger at Congress—Congress should act promptly to give the FBI and other Federal law enforcement the tools they need to rein in fraud and corruption. And we should not let partisanship get in the way of this.

Too often these days, whether it is Senator Whitehouse’s bill to make sure the FBI can respond to requests from local officials to provide help in investigating violent crime, or Senator Blumenthal’s bill to close a gap in the law with respect to the authority of the Secret Service, or our bill to ensure that the U.S. Marshals upon request can provide timely assistance in missing children cases, these seem to be delayed for no good purpose.

I wish we all respected our law enforcement and national security agencies more. I wish we would give them the support they need and deserve. We hear a lot of tearing down of our law enforcement. We should be building them up and giving them the tools they need.

I thank the Director for returning to the Committee, and through him I thank the hard-working men and women of the FBI. I know many of them—not all by any means—but I know they do vital work every day to keep us safe. And, Director, please give my compliments to the men and women of the FBI.

Senator Grassley.

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

Senator GRASSLEY. Thank you, Mr. Chairman, for this very important hearing, and I wanted to inform you that I was not supposed to be here until 10:30 because I was supposed to be on the floor, and when I got over there, they said it would not start until 10:25. So I have to come back here and give my statement. Then I will go back over there, and I will come back for questions.

Chairman LEAHY. In fact, if I might, I told the Director when the first vote starts, I will stay until almost the end of it and then go over. We will keep the hearing going, and Senators can go over and vote and come back, and we will keep it going.

Go ahead.

Senator GRASSLEY. And, obviously, Mr. Mueller, you know there are some questions I want to ask you.

It has been 5 months since Congress passed and President Obama signed into law an unprecedented 2-year extension of Director Mueller's term as Director of the FBI. Given the historical problems with FBI amassing power, the President's request to extend Director Mueller's term for an additional 2 years, breaking from our 35-year practice of limiting the Director to a 10-year term, it was not a decision that I took lightly. Ultimately, given the President's failure to nominate a replacement timely and in a responsible manner, I agreed to the request to provide this historic extension.

I am pleased that Chairman Leahy and members of the Committee agreed with me and moved the extension through regular order, including a hearing, an executive markup, floor consideration, a new nomination from the President, along with a final confirmation vote. This process sets the historic record that extending a Director's term was not a fly by-night decision. It also puts the President on notice to begin the process of selecting and nominating a new FBI Director earlier than the last attempt. Another extension will not occur.

That said, I want to welcome Director Mueller to this day's hearing. His tenure as FBI Director has been a very good one, and his dedication and reputation were significant factors in his 100-0 confirmation vote in July. I am sure that when his 2-year extension runs, he will be looking for the transition, helping other people transition to office, and a well-earned change of lifestyle.

First I want to discuss a perpetual problem at the FBI: whistleblower protection. Director Mueller has repeatedly assured me that

he will not tolerate retaliation against whistleblowers at the FBI. Despite these assurances, two particular whistleblower cases have been dragging on for years. These cases are largely fueled by the FBI's desire to continue to appeal rulings and findings of wrongdoing by FBI supervisors. FBI Agent Jane Turner filed a whistleblower complaint in 2002 when she discovered FBI agents were removing items from Ground Zero following 9/11. She faced retaliation for raising concerns about these agents, and her case has been stuck in administrative limbo at the Justice Department for over 9 years. Nine years is far too long for any case to be resolved, especially a whistleblower case.

Another case, that of Robert Kobus, a 30-year non-agent employee of the FBI who disclosed time and attendance fraud, has languished for over 5 years. Again, the FBI has continued to appeal this case despite clear findings of retaliation.

I wrote to Holder last month about these issues. The response was lackluster. If the Attorney General, the Deputy Attorney General, and the FBI Director truly wished to help whistleblowers, they have the power to end years of appeals. In other words, you do not have to appeal. And there may be reasons other than just money that you are appealing because maybe you hope these people die and go away. I do not think they are going to.

I also want to discuss some issues that have recently arisen as a follow-up the FBI's closing the Amerithrax investigation. The Justice Department recently settled a death lawsuit in Florida for \$2.5 million. The lawsuit raised questions in the press given the potentially conflicting statements made by the Justice Department that seemed to cast doubts on Dr. Ivins' ability to actually manufacture anthrax. Ultimately the Department filed a supplemental brief correcting statements that seemed to cast doubt upon the FBI's case but did not seek to refute the depositions of Dr. Ivins' co-workers.

I wrote to the Attorney General and FBI Director in August asking how the Department's filings and depositions could be squared against the FBI's contention that Dr. Ivins was the sole assailant. While the Department attempts to thread the needle about the Government's liability, the fact remains that the Government ended up paying \$2.5 million to settle the case and cast a further cloud on the FBI's assertion that Dr. Ivins was the sole perpetrator.

I am also concerned about two other issues arising out of the anthrax investigation. First, in responding to press accounts questioning the Government's case against Dr. Ivins, the FBI and the Department of Justice both allowed line agents and attorneys to be interviewed on national television.

Now, pay attention to this because this is another inconsistency between Congressional oversight and what the FBI and the Justice Department is willing to do for other people under other circumstances.

Despite this full and public access to the press that they have given FBI agents on national television, the Department has denied access to line agents as part of our investigation into ATF's Operation Fast and Furious. Now, how do you square that inconsistency? So I want to know from Director Mueller why he allows

line agents to provide detailed interviews to the press on national television but repeatedly refuses to let the Congress and their staff interview line agents and attorneys?

Second, I want to know why the Department of Justice has declined to prosecute the individuals that leaked information about the investigation of Dr. Steven Hatfill. That leak cost the American taxpayers nearly \$6 million in a civil settlement for Privacy Act violations. The American people who picked up the tab for this leak deserve to know the names of the FBI or DOJ employees involved, why they were not prosecuted, and whether they faced any administrative punishment.

I would also like to note that today is the 1-year anniversary of the shooting of Brian Terry. My investigation into ATF's failed Operation Fast and Furious continues. I sent Director Mueller a letter dated October 20, 2011, asking some questions about the FBI's investigation of the murder of Agent Terry. I have not received a response, but I have talked to Director Mueller. He has been very good to come to my office and discuss these cases. I would like a commitment from Director Mueller that my letter will be answered in writing. The Terry family deserves answers about Agent Terry's murder, and answering my letter is another step toward getting those answers.

If we have time during these rounds of investigation, I would like to ask the Director about his involvement in drafting of a memorandum that was reported in the press regarding the targeted killing of al-Awlaki, the potential transfer of known enemy combatant Daquduq from U.S. military custody to Iraq, the FBI's involvement in the investigation of mortgage fraud at Countrywide Financial, and the alleged cozy relationship between mobster Mark Rossetti and the Boston FBI.

Thank you very much, Mr. Chairman.

Chairman LEAHY. With that cheerful welcome, Mr. Director, will you please stand and raise your right hand? Do you solemnly swear that the testimony you will give will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. MUELLER. I do.

Chairman LEAHY. Go ahead, please, sir.

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

Mr. MUELLER. Thank you. Good morning, Chairman Leahy, Ranking Member Grassley, other members of the Committee.

Chairman LEAHY. Is your microphone on?

Mr. MUELLER. I am sorry. Let me start again. My apologies. Good morning, Chairman Leahy, Ranking Member Grassley, other members of the Committee, and thank you for the opportunity to appear today before the Committee and discuss your concerns. I also want to thank you for your continued support of the men and women of the FBI.

Three months ago, our Nation marked the tenth anniversary of the September 11th attacks. The horrific events of that day were the prelude to a decade of political, economic, and cultural transformation, and globalization and technology have accelerated these

changes. And since that time, there have been significant changes in political leadership across the world, including the recent events in Libya and Egypt. And in the economic arena, the past decade has seen billion-dollar investment frauds, the failure of storied financial institutions, and the abuse of financial products which have undermined the world's financial system. There has also been an exponential expansion in the development of new technologies, and these advancements have changed the way we work, the way we socialize, and the way we communicate with each other.

These changes in the global landscape have posed significant challenges to the FBI and our partners in the intelligence community and in the law enforcement community. Accelerated by these changes, the threats to our Nation are constantly evolving, and today's FBI now faces an ever changing threat environment.

Let me begin with the terrorist threat. During the past decade, we have weakened al Qaeda. Due to the coordinated efforts of our military, the intelligence community, law enforcement, and our international partners, we have captured or killed many al Qaeda leaders and operatives, including Osama bin Laden and Anwar al-Awlaki, and we have uncovered dozens of cells and prevented numerous attacks.

Yet core al Qaeda operating out of Pakistan remains committed to high-profile attacks against the West. This was confirmed from the records we seized from bin Laden's compound upon his death. And meanwhile al Qaeda affiliates have emerged as significant threats. Al Qaeda in the Arabian Peninsula, operating in Yemen, has attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009 and the attempted bombing of U.S.-bound cargo planes in October of 2010.

Most recently, we have a growing concern about the threat from homegrown violent extremists. These individuals have no typical profile. Their experiences and motives are often distinct, but they are increasingly savvy and willing to act alone, which makes them increasingly difficult to find and to stop.

We must as an organization, working with our counterparts, keep adapting to these changing terrorist threats, staying one step ahead of those who would do us harm. And we must do all of this while respecting the rule of law and the safeguards guaranteed by the Constitution.

Let me turn for a moment from terrorists to spies. Many people assumed the end of the cold war made the world of cloak and dagger obsolete. Unfortunately, espionage is still very much with us. Nations will always try to learn one another's secrets to gain political, military, or economic advantage. Indeed, the foreign intelligence presence operating in the United States is roughly the same as it was during the cold war. And apart from the more traditional types of espionage, today's spies, just as often students, researchers, business people, are operators of front companies, and they seek not only state secrets but trade secrets from corporations and universities, such as research and development, intellectual property, and insider information.

Turning to the growing cyber threat, the anonymity of the Internet makes it difficult to discern the identity, the motives, and the location of an intruder, and the proliferation of portable devices

that connect to the Internet only increases the opportunity to steal vital information. The number and sophistication of computer intrusions have increased dramatically in recent years. American companies are losing billions of dollars' worth of intellectual property, research and development, and trade secrets. Outside attackers burrow into company networks and remain undiscovered for months or even years. And we must also consider that hostile nations or terrorist groups could launch cyber attacks against our critical infrastructure.

To combat these threats, the FBI has cyber squads in each of our 56 field offices and more than 1,000 specially trained agents, analysts, and forensic examiners that run complex undercover investigations and examine digital evidence.

The FBI leads the National Cyber Investigative Joint Task Force that brings together numerous partners from the intelligence community and other Federal agencies to identify and disrupt significant cyber threats. These efforts have led to successful disruptions of large-scale illegal botnets and transnational hacking schemes involving in some cases millions of computers and millions of dollars.

We also face threats from sophisticated financial crimes as well as health care and mortgage frauds. The FBI and law enforcement partners continue to uncover major frauds, insider trading activity, and Ponzi schemes. At the end of fiscal year 2011, the FBI had more than 2,500 active corporate and securities fraud investigations, a 47-percent increase since 2008. Over the past 3 years, the FBI has obtained approximately \$23.5 billion in recoveries, fines, and restitutions in such programs. And during fiscal year 2011, the FBI obtained 611 convictions, a historic high.

The focus on health care and mortgage fraud is no less important. In 2011, the FBI had approximately 2,600 health care fraud investigations and roughly 3,000 pending mortgage fraud investigations with nearly 70 percent involving losses of more than \$1 million.

Let me just add that public corruption remains among the FBI's highest priorities, particularly along the southwest border. The FBI continues to dedicate resources to 13 Border Corruption Task Forces focused on disrupting the efforts of Mexican drug organizations to corrupt U.S. public officials.

Finally, the FBI continues to work hard to protect our communities from the longstanding threats from gangs and violent crime. We have more than 150 Safe Streets and Safe Trails Task Forces across the country. We target high-level violent enterprises and senior gang leadership to yield the greatest impact prosecutions.

Nor have we forgotten the children. We remain vigilant in our efforts to remove predators from our communities and to help keep our children safe. And we have ready response teams stationed across the country to quickly respond to child abductions.

Now, regardless of the complexity and the evolving nature of modern threats, the rule of law will remain the FBI's guiding principle, as will the protection of privacy and civil liberties for the American people.

Chairman Leahy and Ranking Member Grassley, let me conclude by thanking you and the Committee for your continued support of

the FBI and its mission. Of course, I would be happy to answer any questions you might have.

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

Chairman LEAHY. Well, thank you very much. I am sure that other Senators are probably going to ask you about Fast and Furious, which was not my No. 1 choice to ask, but I have been reading so much about allegations and conspiracy theories that have been aired by some Congressional Republicans, I thought I would ask you a couple questions.

Congressman Issa went on national television and suggested the FBI engaged in a coverup of the crime scene at which Immigration and Customs Enforcement Agent Brian Terry was killed and is continuing a coverup. He suggested that there was a third gun recovered at the crime scene, even that it was the murder weapon, and that the FBI was intentionally covering it up. I believe I know the answer to this, but what are the facts with respect to whether there was a third gun recovered at the scene of the crime, as Chairman Issa suggested?

Mr. MUELLER. Well, let me start with adamantly rejecting the suggestion that the FBI would in any way cover up what happened in the tragic killing of Brian Terry. To the contrary, every available and necessary resource has been put on that and similar investigations where we lose one of our own.

I am familiar with the suggestion that there was a third gun at the scene. There was no third weapon found at the scene. There were two weapons that were found at the scene, not a third. Why there were suggestions as to a third, I am still not certain. It may well be that the two weapons that were found were designated K-2 and K-3 because there was a K-1 that was not a weapon. But the fact of the matter is there were only two weapons found at the scene.

Chairman LEAHY. Also, the Congressman said the FBI is not looking for the killer of Brian Terry. How would you respond?

Mr. MUELLER. Again, to the contrary, there has been one arrest. There is an ongoing investigation. Documents have been filed that are under seal, and there is an ongoing, strong investigation. And we will bring to justice those persons who are in any way involved in the killing of Officer Brian Terry.

Chairman LEAHY. I ask the question only to clear the air, and obviously any one of us who have been involved in crime investigations knows that the less you talk about the steps you are taking, the more effective it is going to be. But I did want those allegations out there. Knowing the answers to them, I thought it would be a good chance for you to be able to state publicly the answer you did, and I thank you.

Now, protecting American consumers and businesses from cyber crime has been a priority of the Committee for many years, and recently the FBI issued a warning about a new phishing scheme in which cyber criminals are stealing American consumers' bank account information. At the same time they are launching denial-of-service attacks on U.S. banks to conceal these crimes. It is not like the old days where somebody would come with a gun into a bank, steal a few thousand dollars, and usually get found quickly there-

after. A study released by the Symantec Corporation estimates the cost of cyber crime globally is \$114 billion a year.

In September, the Judiciary Committee favorably reported legislation that would provide new tools to the Justice Department to combat the growing threat of cyber crime, including a provision that would amend the criminal code to add to violations of the Computer Fraud and Abuse Act the definition of “racketeering” to make it easier for the Justice Department to go after such cyber crime.

So I will ask you first how concerned you are about the growing threat of cyber crime. And would my proposal help the FBI investigate organized crime and cyber crime?

Mr. MUELLER. As I have indicated in my remarks, both my remarks here today but also the longer statement that I submitted, cyber crime is going to be one of the top priorities of the FBI in the future for the very reasons that you articulated and the amount, the numbers of dollars that are lost in a variety of ways. But perhaps a more immediate concern is the possibility of people using cyber skills to attack our National security, whether interfering with the electrical grids or the energy and the like. We have seen around the world countries willing to utilize the cyber battlefield before they launch attacks.

And so for us in the FBI, we have a long-range plan to buildup our cyber capabilities. We have since 2001 roughly doubled the number of personnel that we have on this particular priority. And we have used some innovative ways to address cyber criminals using both the criminal authorities as well as the civil authorities. Making cyber offenses the predicate offenses for racketeering, a racketeering charge, would be helpful—would be both appropriate as well as helpful. And so I believe—I have not had a chance to discuss it with the Department, but my expectation is that the Department would be supportive, as would we.

Chairman LEAHY. It is a long way from the Bonnie and Clyde or Willie Sutton days. You can have a career criminal a few decades ago who might have spent years robbing banks, while the same thing can be done now in a nanosecond.

Mr. MUELLER. And the persons will not be in the city where you are located or the county or the State or even the country. They can be in Turkey or Morocco or Romania or Bulgaria or Estonia or Singapore. And, consequently, the change for us is that we have to develop the relationships to be able to conduct these investigations worldwide if we are at all to be successful in addressing cyber crime.

Chairman LEAHY. I recently introduced a bipartisan Violence Against Women Reauthorization Act of 2011. I worked with Senators Crapo and Kirk and many Senators on this Committee. I know the FBI is currently working to update the definition of rape for the Uniform Crime Report. Why is that important to update that?

Mr. MUELLER. That definition was in some ways unworkable, certainly not fully applicable to the types of crimes that it should cover. And as I think you are aware, the Advisory Committee for NCIC, in developing the statistics, approved a change to that defi-

tion, and my expectation is it will go into effect sometime this spring.

Chairman LEAHY. Thank you. Last, Senator Grassley and I worked together in this Congress on the Fighting Fraud to Protect Taxpayers Act to give the Department of Justice and the FBI additional resources to investigate fraud cases at no cost to taxpayers. It is a good investment. The Vice President announced this week in 2011 the Department of Justice recovered \$5.6 billion in fines, penalties, and recoveries from fraud cases, \$15 billion since the start of this administration. That is a lot more than it cost to investigate and prosecute them. If we can pass the bill that Senator Grassley and I have introduced—it is now stalled in the Senate even though it saves taxpayers money—I suspect we will recover even more. Would the American people benefit—and I realize this is kind of a leading question—but would the American people benefit if the FBI could hire more fraud investigators because of increased resources to target fraud if the Fighting Fraud to Protect Taxpayers Act becomes law? Feel free to answer that any way you want.

Mr. MUELLER. Well, the obvious answer to that leading question is yes.

[Laughter.]

Mr. MUELLER. But whenever it comes to the budget issues and discussions, we have got to prioritize. Certainly white-collar crime in particular, large-scale white-collar crime is one of our substantial priorities.

Chairman LEAHY. Thank you.

Senator SESSIONS.

Senator SESSIONS. Thank you, Mr. Chairman, and I appreciate the FBI. I had the honor to work with them 15 years as a Federal prosecutor. I believe they represent the very finest in American law enforcement, maybe the finest, you would think, I am sure, and I share the view they are perhaps the finest law enforcement agency in the world ever seen. They are highly paid. We have increased the numbers. We have provided them technical support and training the likes of which few agencies in the world can match, and certainly not in the numbers that we have seen before.

So we expect a lot out of the FBI, and I believe your background as a prosecutor and having worked with the FBI for many, many years provided you the kind of experience necessary to be a good Director.

I would just say with regard to your letter of November 24th on mandatory military detention, I thought you overstated the case but raised some points of importance. The legislation in conference was altered. It is clear to me—let me just say this: I am absolutely convinced that the right policy is to presume that combatants against the United States will be held in military custody, but I absolutely believe the FBI should participate in those investigations. So we added language that said, “Nothing in this section shall be construed to affect the existing criminal enforcement and national security authorities of the FBI with regard to a covered person, regardless of whether such covered person is held in military custody.”

Does that answer at least some of the concerns you have to make clear that the FBI might continue to participate in investigations in which your ability and skills would play an important role?

Mr. MUELLER. Senator, you might understand that I would disagree on the characterization that I overstated it. I would say that I stated it appropriately in that letter, my concerns with regard to the NDAA. And there were two basic concerns.

The first was the adverse impact on our authorities or the lack of clarity with regard to our authorities. And the language that was developed goes a long way to resolving that particular issue, and it tends to assure us that our authorities will be maintained.

The other concern I voice in the letter is the uncertainty that the statute raises with regard to what happens at the time of arrest, and as I know you know, having been a prosecutor, it is tremendously important at the time of arrest that you make the right decisions in terms of addressing the person, particularly persons whom you hope to cooperate, not just interrogate but to cooperate and turn around on others. And the statute lacks clarity with regard to what happens at the time of arrest. It lacks clarity with regard to what happens if we had a case in Lackawanna, New York, and an arrest has to be made there and there is no military within several hundred miles. What happens if we have a case that we are investigating on three individuals, two of whom are American citizens and would not go to military custody and the third is not an American citizen and could go to military custody?

Now, in my discussions with others, I understand the answer to be, well, the President can waive this provision; or, second, procedures are going to be developed that will satisfy that uncertainty. And my continuing concern is that that uncertainty will be there until it is resolved in some way, by statute or otherwise.

If I may just add one other point—actually, two points. I am as interested as anybody in developing intelligence to prevent attacks because if there is an attack, the person they are going to look to sits here. What I am concerned about, however, is long term as well. This statute that gives the military an inroad to making detentions in the United States may be applicable and work well with the persons you have now. But 5 years or 10 years down the road, what could this mean?

And so while the changes in the statute have addressed some of my concerns, the changes have not—and I appreciate it—they have not addressed all of my concerns.

Senator SESSIONS. We disagree. To me, there is no rational argument that can be made that would suggest the United States is not in a better legal position to treat an al Qaeda member arrested in the United States as they are, a military combatant, with the full ability of the FBI to participate in the investigation. Giving Miranda warnings, presenting them to courts in very short order, providing them with lawyers within hours of arrest, allowing them to make phone calls to their co-conspirators that civil law prosecution requires is not helpful in a war. So that is where we disagree, and I will go to the next question.

Mr. MUELLER. May I just clarify one thing?

Senator SESSIONS. All right.

Mr. MUELLER. What I have focused on is what happens at the time of arrest, and—

Senator SESSIONS. Well, listen, you need to work this out with the Department of Defense, don't you—

Chairman LEAHY. Let him answer the—

Senator SESSIONS. Well, I want to—my time is about up.

Mr. MUELLER. I just want to say that the focus—

Senator SESSIONS. I let him talk.

Mr. MUELLER. I just wanted to make certain that you understand that my focus is on the uncertainty that happens during that period of time, at and about the time of arrest, and what happens afterwards, particularly when we have been successful getting people to cooperate.

Senator SESSIONS. Yes, I certainly agree. I think that is what the purpose of this was, presumptively treat them as a military detainee and then to have memorandums of understanding or cross-designations that would allow full participation. But maybe this language will help you there. I appreciate you sharing that.

With regard to the Chairman's talks about fraud and prosecutions, I got to tell you, I am disappointed in the decline of those prosecutions. This chart shows some of the cases and their declines. We have had some progress in some of the cases, but bank embezzlement went from 230 in 2006 to 130. Financial institution embezzlement went from 31 to 17. Financial institution fraud went from 752 to 570. Bankruptcy fraud stayed about flat. Bank robbery prosecutions down significantly. In a time when the American people are concerned about the financial integrity of some of the businesses that are failing—and it does appear many of them have had wrongdoing as a part of that—are you concerned that we are not adequately addressing it? And I would note—and I will ask you maybe in written questions—that your numbers look a lot better. But to me, I have always felt the Administrative Office of the Court's numbers represent a more accurate number than agency numbers. So your numbers do look better than that, but I think these are the ones that represent people actually charged and actually convicted.

Mr. MUELLER. Let me just respond to the last, because we want to correlate those numbers. We in no way wish to fudge the numbers, and you will see in a number of categories the numbers going down, particularly since 2001 because we had to prioritize.

Senator SESSIONS. Well, this is from 2006 to 2011.

Mr. MUELLER. And I will tell you there is not an FBI agent who joined in the last 15 to 20 years who does not love doing bank robberies. But the fact of the matter is we cannot afford to do the same number of bank robberies and embezzlements that we have done in the past because of the demands of terrorism, gangs, cyber, cyber intrusions—

Senator SESSIONS. Well, bank robberies—I understand the argument. That has been going on for 25 years—

Chairman LEAHY. The Senator's time has—

Senator SESSIONS [continuing]. But the other ones are more—

Chairman LEAHY. The Senator's time has expired, and as I said earlier, I am glad to see the Department of Justice has recovered

\$5.6 billion this year alone through fines, penalties, and recoveries, \$15 billion so far in this administration.

Senator KOHL.

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

Director Mueller, the FBI has proposed closing three of its six Wisconsin satellite offices. If these closures go through, the Western District of Wisconsin will be especially hard hit and will lose half of its FBI offices. As I told General Holder and I wrote to you last month, I have strong objections to these closures. You have indicated that Wisconsin will not lose agents or resources, so this clearly is not a simple cost-saving issue, and we think it is a bad idea to close these offices.

As I have heard from law enforcement throughout the Western District in Wisconsin, FBI presence in these semi-rural areas is critical to maintaining long-term partnerships that protect Wisconsinites from criminal and terrorism threats.

Now, you have long emphasized to our Committee the importance of the FBI's coordination with local law enforcement, and you have stressed that the FBI must maintain close contact with the law enforcement officers who are on the street day in and day out, working "shoulder to shoulder" with them.

How are these closures which would move FBI agents hours away from large cities like Wausau and La Crosse consistent with the statements that you have made about working shoulder to shoulder with local law enforcement?

Mr. MUELLER. Well, the broad view is, Senator, we have 56 field offices and just less than 400—I think it is about 385, 390 resident agencies around the country. And the fact of the matter is we have undertaken a review for the last 2 years on all of our resident agencies to determine if they are the most effective way of providing the support to State and local law enforcement, which is tremendously important, as you indicate.

I did go back after the last hearing and look at the issues relating to these resident agencies, and I do believe that there are cost savings, particularly with regard to the necessity for outfitting our resident agencies with SCIFs where classified information can be maintained. It is very expensive to rent the space and put in the capability of a resident agency to handle classified information. And so, yes, it does go to cost.

What we have tried to do is look at the threats in the Western District of Wisconsin and determine how best we can address those particular threats, understanding that the personnel who were in these other two resident agencies would be in the other resident agency that is in western Wisconsin.

And so I would like nothing better than to tell you, Senator, I agree, we are going to keep them; but in reviewing the situation, I do agree that the decision is appropriate to consolidate those resources in a particular resident agency where we can better prioritize, make some savings, and my hope and expectation is provide exactly the same degree of service that we had before.

Senator KOHL. I understand that there are a total of 26 office closures being proposed all over the country over the next 2 years, and three of them are in Wisconsin. Can you provide me a list of the other 23 proposed offices to be closed?

Mr. MUELLER. I think I would have to get back to you on that. I presume we would be able to, as long as other notifications have gone out.

Senator KOHL. Thank you, Director Mueller.

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

Senator KOHL. As I stated earlier, and often, and here today, I object to these closures in Wisconsin. Now, I understand that you have already signed off on them, but I hope in the spirit of open-mindedness you will continue to work with me and to consider the possibility that maybe we can do better in Wisconsin in serving the people of Wisconsin. I know you are an open man. You have indicated that time and time over your tenure. So while the issue is said to be closed, I would like to hope that it is not finally and irrevocably closed.

Mr. MUELLER. There is a crack there.

Senator KOHL. All right. Thank you.

[Laughter.]

Mr. MUELLER. I am always open to additional arguments. Anytime before something happens, I can be—if I see I am making the wrong decision, I try to entertain the information and make the right decision. So I would welcome what other information or whatever you want to provide.

Senator KOHL. Well said, and I appreciate that.

Mr. MUELLER. Yes, sir.

Senator KOHL. Director Mueller, last week this Committee passed a bill that I authored to increase the maximum sentence for economic espionage, which, of course, is the theft of trade secrets for the benefit of foreign countries, and to direct the Sentencing Commission to consider increasing the sentencing range for trade secret theft and economic espionage. This is an important step to stem a surge in crime that costs United States companies billions of dollars each year, and I look forward to its swift passage.

As you know, when companies fall victim to trade secret theft, they are often reluctant to share details of the theft with the Government for fear that if the theft becomes publicly known at the investigatory stage, it will harm their reputation and bottom line. But if the FBI, on the other hand, does not know about the theft, it cannot investigate and help other companies guard against these threats.

Director Mueller, what steps are you taking to improve your relationship with the private sector to assure them that their information will not be exposed unless or until the Government decides to prosecute the case? What efforts are you taking to bring more economic espionage cases?

Mr. MUELLER. Well, in terms of the economic espionage cases, we have had some substantial ones. Several of them I think are listed in my longer statement where we have arrested and successfully prosecuted individuals who have stolen secrets from various corporations. One large case, agricultural entities where an individual had stolen a well-recognized biologist's—stolen their secrets and was in the process of taking them to China where we interceded and successfully arrested the individual and successfully prosecuted him. And there have been a number of these particular cases.

We appreciate the enhanced sentencing. Enhanced sentencing transcends into enhanced deterrence. With regard to working with the private sector, I would say that it is much like the issues relating to a data breach where companies would be reluctant to inform us of intrusions because of the impact on those companies. We work very closely through a number of outreach programs that we have in every one of our districts to assure the corporations and business leaders in that particular community that there are ways of keeping their secrets private. We can go in and get a court order that maintains that privacy. But it is absolutely imperative that we know what is happening in order to be able to stop it, and if it is in your company, it may be in another company, and you have to let us know what is happening if we are to protect not just your company in the future but other companies that may be adversely affected as well.

Senator KOHL. Thank you.

Thank you very much, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Senator Grassley.

Senator GRASSLEY. Yes, thank you, Director Mueller, for coming.

My first question is about the letter authorizing the targeted killing of Anwar al-Awlaki and another U.S. citizen. The reason I ask this question is I am getting a lot of mail from Iowans wanting to know the authority for the United States to take that action, and I assume this letter gives that authority.

Do you support Congress having a copy of that letter?

Mr. MUELLER. It really is not my—sir, it is not my role. It is—whatever may have been developed would be developed by the Department of Justice. We would not have played a role in it. Some of our information may have been used if there was such a finding. But I ask that you perhaps direct that to the Department of Justice.

Senator GRASSLEY. The Department of Justice settled a civil lawsuit for Dr. Hatfill for violation of the Privacy Act for leaking details of the investigation. It cost the taxpayers \$6 million in the settlement. I have repeatedly asked both the Department as well as your agency to identify the individuals who leaked information on the investigation. I have been repeatedly told the investigation is ongoing, and I assume that is the excuse for not answering our information we have requested.

In response to an August 31, 2011, letter on the anthrax attacks, the Department of Justice informed me that the investigation is complete and that no criminal charges will be filed against those who leaked the information.

I have three questions. I will give you all three of them. Were the individuals who leaked FBI agents or employees of the FBI? What, if any, administrative action did you take against these individuals if they were FBI agents or employees? And do these people still have their jobs if they are FBI employees?

Mr. MUELLER. Well, Senator, I appreciate your discussing this with me. These questions are more specific than the ones you raised when we met, and I would have to get back to you on it because it is specific to the FBI. I know there were other entities other than the FBI and the Department of Justice that had under-

taken an investigation as well. So I will have to get back to you on that. And to the extent that the investigations were undertaken by entities in the Department of Justice, I would defer to the Department of Justice in terms of providing information. But to the extent that it is specific to the FBI, I would have to get back to you on those questions.

Senator GRASSLEY. My next question deals with sensitive interactions between the FBI and other law enforcement agencies, and you probably know that sometimes you get accused—your agency does—of not playing well with other law enforcement agencies. I am sure you would agree that if we are busy fighting each other, then we are not fighting our real enemies.

Recently, I have seen news articles about infighting between the FBI and New York police. I was especially bothered by press reports of the FBI sources pointing out weaknesses of the New York Police Department terrorism case. At the same time, I am hearing complaints about the FBI's inability to cooperate with the Department of Homeland Security OIG in border corruption investigations. These complaints sound as if the FBI is using kind of a Pac-Man mentality.

Since the culture of an organization starts at the top, I am concerned about what may be going on in management at the FBI. So I want to assume that you would agree that FBI agents should not anonymously or publicly attack the New York Police Department. I am sure that you are committed to having the FBI work with all appropriate partners in addressing border corruption.

So this question: What are you doing to improve the FBI's working relationship with other law enforcement agencies? And how are you relaying that message to line agents and supervisors? And whether it is by impression or whether it is fact, it does not matter. There is a feeling out there that it exists, so it is a problem for you.

Mr. MUELLER. Well, it is. I confess it has been a long-term problem with the FBI. In the wake of September 11th, we identified ten priorities. Eight of them were programmatic priorities, as you can imagine: counterterrorism, counterintelligence, and cyber; and then on the criminal side, public corruption and the like.

The ninth priority was collaboration with our Federal, State, local, and international partners. And there were only ten priorities, and the significance of that is that we understood that we could not be successful by our own, that our success is dependent upon our partnerships. And since September 11th, since I have been there, I think we have made substantial strides in working with State and local law enforcement. And if you do talk with the IACP, International Sheriffs, or a number of the organizations, Major City Chiefs, my hope is and expectation would be that they say there has been a substantial change and we work very collaboratively.

I was as distressed as you and others to see the press reports, anonymous, of Federal Government persons talking about another prosecutor's and another agency's investigation, this being NYPD. I gave directions that that should not happen, and when I saw it happening, I again went back to give directions to have it stop. I had Sean Joyce, who is the Deputy, talk to Ray Kelly. I had talked to Ray Kelly. He gave me a call, and we have discussed this. It

does not interfere—we understand it should not have happened. From our perspective it should not have happened. But we still have a very good relationship with NYPD, particularly when it comes to addressing terrorism.

We recognize, I recognize that Ray Kelly has done a remarkable job in terms of protecting New York City from terrorist attacks, New York City being a principal target. And as I say, these things are unfortunate. I wish they did not happen, but our relationship remains solid.

Second, with regard to what is happening on the border in terms of the handling of public corruption cases within the DHS agencies, we seek to work with those partners that want to work with us in developing these cases. And we leave it up to the Department of Homeland Security to sort out the counterparts with whom we should work, understanding that public corruption on the border is a substantial issue and those cases have to be addressed, and they have to be addressed swiftly. And we seek to do it with the Inspector General's office or the Internal Affairs, whichever entities would join with us in addressing that form of public corruption.

Senator GRASSLEY. Thank you.

Chairman LEAHY. Thank you very much.

Senator Feinstein.

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

Mr. Mueller, as you know, I have known you for a long time.

Mr. MUELLER. Yes, ma'am.

Senator FEINSTEIN. I think the FBI is very fortunate to have your leadership. You have always been a straight shooter. I think your credibility and integrity is unmatched, and I just want to say that.

As you may know, ICANN, the Internet Corporation for Assigned Names and Numbers, which governs top-level Internet domain names, is planning to open these wide effective January 12. Names will go beyond .com, .mil, .edu, .gov, and the other established extensions to virtually anything, .gap—and the gap is very concerned—.sex, .disney, .bomb, anything.

Do you think it would be advisable for ICANN to delay this extension so Congress and others can take a closer look at this situation, evaluate its implications for United States consumers, United States businesses, and, most importantly, Internet security?

Mr. MUELLER. Senator, I have not looked at this in some time, and what knowledge I have is somewhat passing. My impression is that it opens up a can of worms, and we do not know exactly what is going to happen as a result. So any effort to analyze and to in my mind constrain the different uses to which this could be put would be valuable. I understand, however, that ICANN has been a product principally of the United States or is an entity supported principally and agreed to by the United States and certain countries, but there is a desire out there to break the hold. So it may well be an uphill battle, but any effort that can be made to look at and anticipate what is going to come out of this would be, I think, beneficial.

Senator FEINSTEIN. Well, another way of doing it—and I thank you for that—is to stagger what they can do at any one time so you

do not have literally hundreds or thousands of new domains appearing all at once with all kinds of mischief.

Mr. MUELLER. Let me ask you this, if I could get back to you and talk to Sean Henry—

Senator FEINSTEIN. Would you, if you would?

Mr. MUELLER [continuing]. And get his impact. He is the expert in this area, and we will get back to you and see what thoughts we might have on that particular issue.

Senator FEINSTEIN. If you could, I would appreciate that.

Mr. MUELLER. Yes, I am happy to do that.

Senator FEINSTEIN. As you know, when you first began to develop a National Security Division and go into the intelligence area, I doubted whether it could be done efficiently and effectively. I believe you have done it. I think the record indicates that. I think the intelligence, I think the way the 56 offices operate, I think the fact that you have made 400 prosecutions as opposed to six military commission trials has demonstrated that the FBI has been effective.

As you know, the defense bill will have a military presumption in it, it looks like. Many of us on this side of the aisle do not believe that is the way to go, that there ought to be flexibility for the administration to say the evidence in this case best suits itself for a Federal prosecution, the evidence in this case suits itself for a military commission, and have the ability to make that decision.

I have never asked you, at least, for your view on this. Could you talk a little bit about this and why you believe that this flexibility is so important?

Mr. MUELLER. Well, as I indicated in response to questions from Senator Sessions, when the bill first came out and we looked at it, I had several concerns and expressed those concerns in a letter to the Armed Services Committee. The two concerns were: first of all, what impact it might have on the continuing use of our authorities; and then, second, it created uncertainty as to what happens at the time of arrest, particularly at a critical time when we are trying to get a person to cooperate.

Now, the legislation talks about not interrupting interrogations, which is good, but gaining cooperation is something different than continuing an interrogation. And my concern is that you do not want to have FBI agents and military showing up at the scene at the same time on a covered person, or with a covered person there may be some uncovered persons there with some uncertainty as to who has the role and who is going to do what.

The answer, as I understand, in the legislation is, well, procedures are to be developed by the administration. Procedures can change. Procedures can be controversial. And to a certain extent, to the extent that the statute introduces uncertainty, that is problematic for us. And to the extent that the uncertainty is to be resolved by procedures, procedures can change. And they can change if you have somebody different in a particular position within the Government that can exploit procedures where they cannot exploit a statute.

So my concern comes in resolving that uncertainty, and I am not certain that the drafters of the statute went some distance in re-

solving the issues relating to our authority with the new language, but did not really fully address my concerns about what—

Senator FEINSTEIN. Because I have been told that you are satisfied with what has been worked out.

Mr. MUELLER. I was satisfied with a part of it with regard to the authorities. I still have concerns about the uncertainties that are raised by the statute, and my understanding last week is that there were some suggestions as to fixes that could be proposed in terms of resolving that other concern that I addressed in my letter.

Senator FEINSTEIN. Could I ask that you get your specific concerns to us? Some of us are working on a bill in this area, so it would be very useful to have those.

Mr. MUELLER. Well, I did articulate the second part of my letter. The first part related to the authorities. The second part related to the concerns I have about what happens at the time of arrest. And so I have put that in the letter, but I will go back and see if we can—see if there is a possibility in conjunction with the Department of fleshing that out some.

Senator FEINSTEIN. I appreciate that. Thank you very much.

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

Senator FEINSTEIN. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Senator Whitehouse was next, but Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman. Thank you, Mr. Director, for your service.

Mr. Director, millions of Americans have smartphones with pre-installed software designed by a company called Carrier IQ. Recent research has shown that it captures a broad range of sensitive information—

Chairman LEAHY. If the Senator would yield just a moment, I should note Senator Whitehouse went to vote so he could come back to continue the meeting going.

Please go ahead.

Senator FRANKEN. Recent research has shown that Carrier IQ's software captures a broad range of sensitive information like the content of text messages, the content of searches, even if those searches are—if the user thinks they are encrypted, Carrier IQ gets them back unencrypted; also the full addresses of the websites that users use or visit.

News reports have suggested that the FBI accesses and analyzes information gathered by Carrier IQ's software. What wireless carriers has the FBI requested this information from? And what information have you obtained from those requests?

Mr. MUELLER. Let me start off by saying we have neither sought nor obtained any information from Carrier IQ in any one of our investigations. Let me follow up by saying that there was some confusion, I believe, in terms of the response to a Freedom of Information Act request which indicated a standard exemption was being utilized, and from that it was extrapolated that perhaps we were obtaining information from Carrier IQ. As I said before, we are not, have not sought and do not have any information from Carrier IQ.

Senator FRANKEN. Not directly from Carrier, but what about from the wireless carriers?

Mr. MUELLER. That is very general in terms of wireless carriers. I am sure—well, let me put—

Senator FRANKEN. Did you get information from them from the use of their software of Carrier IQ?

Mr. MUELLER. No, I do not believe so. If you are specifying the use of the Carrier IQ software by a wireless carrier, have we sought that? I do not believe so. In other words, I would have to—I would have to check and be more specific in the question and the answer I give you because—

Senator FRANKEN. Can we follow through with that?

Mr. MUELLER [continuing]. Whether it be FISA Title III, we would seek particular information. I do not know any information that we seek from wireless carriers or what have you, and I am not talking about Carrier IQ. I am talking about wireless carriers that we may obtain information that in some way Carrier IQ may have been involved with. I would have to get back to you specifically on that particular question.

Senator FRANKEN. Great. I appreciate that.

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

Senator FRANKEN. In January, the FBI will roll out a facial recognition service in four States. That service will allow State and local law enforcement agents in those States to use a photo of a criminal suspect the way they use fingerprints right now to see if that photo matches up with people already in the system.

What protections will the FBI have in place to make sure that innocent people are not added into this database and to make sure that this service is not used for non-law enforcement purposes?

Mr. MUELLER. Well, this service is going to be used solely for criminal law enforcement and booking photos and the like. It will be made available to other law enforcement in the same way we provide other data to law enforcement, but we will ensure that they are to be used only for approved criminal law enforcement purposes.

Senator FRANKEN. OK. Well, as you roll out this service, I would appreciate it if your office would keep our office up to date on this.

Mr. MUELLER. Happy to do that.

Senator FRANKEN. I would just like to follow up on Senator Feinstein's point, just to ask you to also keep me in the loop on ICANN and their plan to greatly expand these numbers of top-level domains.

Mr. MUELLER. Happy to do that.

Senator FRANKEN. I think that is an issue that might affect the agency's ability to fight Internet fraud and identity theft, et cetera.

I would like to ask you about reports of virulently anti-Muslim statements in some of the FBI's training materials. I am worried that this will further set back the FBI in its efforts to partner it with the Muslim American community to fight terrorism.

Has the FBI issued a clear and unequivocal apology to the Muslim American community for the bigoted and inflammatory statements found in those materials? And would you do so now?

Mr. MUELLER. We have met with various of the representatives of the Muslim community and not only said we apologize for what had happened, but also explained to them the process that we are undergoing to address this issue. It came to our attention last sum-

mer that there may have been inappropriate materials in the course of our training. In the wake of that, we put together a panel of individuals, two from the FBI, three from outside the FBI. The ones outside the FBI have credentials that—one was at West Point, one was at the Naval Academy. But they have credentials at Harvard—not Harvard—Yale, Princeton, and Johns Hopkins. They are outside the FBI with two persons from the FBI who have credentials in the same arena, and they put together a document, a touchstone document that would be the base document for any of our training when it comes to addressing the counterterrorism, particularly when it relates to Muslims.

After putting together that document, we pulled together all of our training materials since September 11th, approximately 160,000 pages, and have gone through and reviewed those materials with the context being how does it relate to the document that these outside and inside experts put together. And then in response to FOIA requests, we have been producing those documents to the public.

Yes, we did have materials in these documents that were inappropriate. They did not represent in any way, shape, or form the FBI's perception. It is tremendously important that the Muslim community cooperate with us, and the Muslim community in many of these prosecutions has been the entity, individuals from the Muslim community have been the ones that alerted us to the issues. And I would say overall I believe our relationship with the Muslim community is very good.

Things like this, as you indicate, set it back, but I do want to assure that we are addressing it, and we are addressing it comprehensively, and it does not represent the belief of the FBI.

Senator FRANKEN. It is an anomaly.

Mr. MUELLER. It is an anomaly. A perfect word to address it, yes.

Senator FRANKEN. Thank you for validating my use of "anomaly."
[Laughter.]

Mr. MUELLER. Thank you.

Senator FRANKEN. And for your service.

Senator WHITEHOUSE [presiding]. Director Mueller, let me jump in and take us back to the cyber issue.

Mr. MUELLER. Yes.

Senator WHITEHOUSE. We are being attacked across the Internet in a whole variety of different ways. We have the sort of light-of-day theft and piracy of intellectual property—movies, music, goods, electronic games—that is rampant around the world. We have direct fraud and theft against individual Americans and businesses. We have what you might call the "brain drain" of intellectual property that is stolen, very often without the knowledge of the company, out of their computers and exported, it appears, primarily to China so that they can compete against our manufacturers without licenses and without R&D expense. And it appears to be national policy on their part to do this. And then, of course, you have the danger of sabotage through the cyber vector, either of our critical infrastructure, our banks, our electric grid, and of military technology that could be disabled or interfered with.

You stack all of that up, and I think there is a case to be made that this may be the greatest transfer of wealth through theft and

piracy in the history of the world, and we are on the losing end of it.

So I am concerned about the resources that we dedicate to this. I understand that you are dealing with budget constraints; you are dealing with an OMB that is primarily concerned about budget, not your outcomes. But what I am hearing back from the private sector folks who are involved in network security and who engage with your agency all the time is that your capability is extraordinary. The people who are involved are absolutely first rate. Organizations like the NCIJTF are operating at the highest level of professionalism. If America could get behind the classified screen and see what they were doing, people would be really proud and impressed.

So the capability is great, but the capacity is what two recent folks said to me, “woefully inadequate,” that there has been one Coreflood case which was a great case, but there could have been a dozen because the problem that Coreflood went after of botnets is profound. It is all over the Web. You mentioned a variety of cyber prosecutions for intellectual property theft. I am not aware of one of them that is a pure cyber case. I believe that they all involved an individual who actually appropriated, expropriated intellectual property. And yet you see—I had a CEO of a major American energy innovator tell me that when he announced a new product, he got hit by 60,000 attacks in the next 2 hours, his company did. We have had one of our major defense contractors have the plans for an entire joint strike fighter hoovered out of their electronic records. We have been briefed about an American company that had a huge investment in a new product that is gone, and there is actually a facility that is being prepared to make that product. Again, no license, no R&D, just stole it from the company.

So I am concerned that we do not yet have the right model for dealing with this in terms of capability, and I have spoken to Jack Lew and to Dana Hyde at OMB, and they are willing to open up to a discussion that would look into how we might better pursue this. You know, should it be its own organized crime strike force model from the Kennedy era? Should it be akin to OCDETF, which has been quite successful against domestic narcotics trafficking? Should it be a new DEA or ATF or FBI? Should it be that big when you consider the scope of the threat and the complexity of making these cases, the forensics of putting together the case, the international angle to virtually all of them, the complexity of the statutes?

I mean, you stack it all up, and each one of these cases is an almost majestic accomplishment to pull it together. And if we are going to do a lot of them, which we need to do, we have got to, I think, throw more money at the problem. And how we best do that I think is a discussion that we need to have, and I would like to ask you if you would be prepared to join in that discussion and let me know who the right person to participate in that discussion for the FBI would be, kind of brainstorming what should this look like for the coming century, because it is not clear that the existing model just accreting a few more agents here or a few more agents there is where we want to end up.

Mr. MUELLER. Let me talk a little bit about where I think we need to go. There are several steps that we are taking to position ourselves to address this phenomenon. The first is—

Senator WHITEHOUSE. You agree it is enormous, it is massive.

Mr. MUELLER. Enormous. It is massive. And there has to be triage, and there has to be prioritization, but there has to be additional resources that are directed to it.

One of the base things we are doing is upgrading the capabilities of every one of our agents by having a basic cyber training so that it brings everybody up to a level to handle much of the cyber crime or that which has migrated to the Internet with sufficient understanding and background in the cyber arena, a baseline for every one of our agents.

Second, to add and to continue to grow with persons who have the backgrounds in this arena, an agent cadre.

Third, internationally. I was in Romania and Bulgaria last week. Both areas, particularly Romania, it is known for its widespread Internet fraud. We have specialists over in Romania at this point. I have got two persons, one that used to be an IBM programmer, the other one worked for a number of software companies, and it extends our reach to our counterparts in the Romanian and the Bulgarian services. We have persons in Estonia, I think in Latvia, and a number of other countries where we have expanded internationally in order to address these crimes.

Internally, the structure of the FBI does not lend itself to easily addressing cyber. Yes, we have a Cyber Division, but what we find, when it comes to espionage, it is now cyber, and the information is exfiltrated as opposed to getting an intelligence officer, getting him in and getting him latched up with people. It is cyber.

Senator WHITEHOUSE. The era of microfilm is over.

Mr. MUELLER. It is still there. People use—they do not want to lose their old ways. We are the same way. But if you are sitting back in one of these countries and you are saying, “Where can I get the biggest bang for my buck?” it has got to be in exfiltrating the information without risking people overseas.

And so what we are looking to do is build on the concept of the NCIJTF, which is threat focus cells. As you know, the principle there is you take an intrusion and you bring your best people to address it, not knowing whether it is going to be espionage or a crime, whether it is going to be a high school student, and then decide how you are going to treat it, whether you are going to treat it as a crime domestically, whether you are going to treat it as a national security risk to be addressed by other agencies in the intelligence side. And that concept of the NCIJTF in my mind has to grow to address cyber crime, because you cannot address it as we have crimes in the past where we have organized crime, we have narcotics, we have public corruption and the like, because it cuts across all those.

So organizationally, we have got to change and buildup our capabilities. Building up the specialists such as the persons that we have over in Romania and Bulgaria now is tremendously important. And we have to find better ways to be more efficient, particularly when it comes to the forensic areas. And as you know, being a United States Attorney, backlogs in terms of forensic capabilities

often hold up prosecutions. We have to become more efficient when it comes to utilizing the forensics to translate what we have forensically into the courtroom and putting people away.

That is generally the direction that we are going in. I would be happy to both myself talk with you and also have Sean Henry, who basically oversees this side of the house, sit down with you and discuss additional areas.

Senator WHITEHOUSE. Good. Well, I have talked to some of my colleagues on the other side of the aisle. They are equally interested in participating in this and trying to figure out where the choke points are, what the best structure would look like, and then I think we have got—it is a big enough problem that I think we need to figure out what the proper design should be for going after it and then worry about how we pay for it, because, frankly, if, in fact, we are on the losing end of the biggest transfer of wealth ever through wealth and piracy, then paying for stopping it is a 1,000:1, 10,000:1, 1,000,000:1 payback. It is really a big deal. I have heard numbers as high as \$1 trillion a year as estimates of what we lose in intellectual property that is just siphoned away, often unbeknownst to the factory or chemical plant or whoever it is that feels that they have adequate security.

In terms of the numbers that we do have—I am going to keep going for a little while because I think some of my colleagues are coming back from the vote, and I will turn it over to them as soon as they return. But while I have you, I would like to pursue this a little bit further with respect to the FBI's own numbers.

When you describe that an agent is headquarters Cyber Division personnel or in the computer intrusion program or in the cyber crime program, does that mean that they are full-time absolutely only dedicated to cyber? Or is this a little bit more like—on the DOJ side, they will report how many cyber AUSAs they have, but having been a U.S. Attorney, I know perfectly well that those cyber AUSAs are probably doing other cases. They are just the ones who have to listen to the conference call with the mute button pushed while they are preparing their gun case or their drug case or whatever, but they are not really a full-time, cyber-only, dedicated member, you know, prosecutor. How does the FBI's count work for that? Do you count your cyber people people who are designated if a cyber case comes up but they are working bank robberies, terrorism, whatever else while they are in between cases?

Mr. MUELLER. Well, nobody is in between a cyber case now. I mean, there is so much work to go around, rarely do you find that. I would have to look at—

Senator WHITEHOUSE. If you count an agent as a cyber-dedicated person, the agent is 100 percent cyber?

Mr. MUELLER. Well, 90 percent. I mean, they have additional duties. They may have SWAT duties, for instance, that kind of thing. But in terms of their caseload, it would be a cyber caseload, and each of the special agents in charge are desperate for additional persons for their cyber squads.

I am not certain what statistics you are looking at, but we have doubled the number of agents who are doing cyber cases since 2001. That is still less than 1,000. But we are—

Senator WHITEHOUSE. Yes, compared to, say, nearly 5,000 DEA agents, nearly 2,500 ATF agents, approximately 3,200 Secret Service agents, over 1,400 postal inspectors, and over 1,200 NCIS agents—all who are doing great work, all who I am very proud of, but when you put those numbers side by side and match it against the cyber problem, there is a disconnect.

Mr. MUELLER. Well, I think we are one of the agencies—the Secret Service quite obviously does, but we have separate cyber career paths. We recruit and bring in agents for the cyber program into new agents class. They get the foundational instruction as to how to be an agent, how to conduct interviews, be an agent, the same way the military will bring somebody in, well, you are army first and then your secondary will be artillery or tanks or something like that. For us, we bring them in, you will be an agent first, but you have particular qualities. You were a software programmer before. I do not want you to do narcotics cases. I want you to do—you are in here to be in the cyber program. And we put them in generally a smaller office for a period of time, but in the cyber arena, and then they will graduate to a larger office.

We have a number of cases, a number of capabilities now where we have persons with special expertise that may be living in Cleveland or San Diego or Portland, Oregon, or Portland, Maine, whom we will bring in on a virtual case, coordinated by headquarters, but where the expertise is around the country, and the bad guys can be anywhere. And for us to be effective down the road, we are going to have to make use of those specialties, regardless of where the individual lies, because the crime is most often not a local crime, not a State crime, but a crime that is launched overseas. And we need to bring the expertise to developing that and allow that group of persons, wherever they are in the United States, to bring the case to a successful close.

Senator WHITEHOUSE. And, first of all, let me just make clear that I very much applaud the direction that you have been going in. I think that within the resources and structure that you have been provided, I am very laudatory of the focus and the professionalism and the additional resources, particularly as you have been constrained and had the terrorism responsibilities added all at the same time. So I do not want to in any way have anything that I have said be taken as a criticism of you or the FBI management. I think it is Congress' job to make sure that you have the resources and the structure that will be most effective to accomplish your mission, and that is a discussion that we need to be having in a different way here in the Congress.

Let me ask you one more question about these cyber cases and where in the array of cases that the FBI engages in they rank in terms of their resource intensiveness and their agent intensiveness. It strikes me that between the subject matter expertise that is necessary to deal in this specialized area, between the computer familiarity that is required and the forensic computer capability to pick apart the actual traffic of what was done where and understand it and be able to bring it out of the code and make it real for prosecutors, for instance, who have to make the case, dealing with the fact that the vast majority of this crime has an overseas component to it, if not being primarily directed from overseas, which means you

have to deal with intelligence services and with legats and with foreign treaties and with—and it is probably a complicated racketeering type case to begin with. So you add it all up, and it strikes me, as a guy who used to have to run these kind of cases, that this is the sort of thing that I look at and think, “Oh, my God, I am going to have to put an awful lot of people on this one to get it done right. This is about as complicated as it gets.”

Is that your take on this as well?

Mr. MUELLER. It really depends on the case, and one thing that I do believe should not be lost in this is that often sources, human sources, are as important as anything else. When you talk cyber, you think about that person with the software development expertise that you need to do the kind of investigative work. But often in these cases it is a combination of cyber and also sources, so we cannot forget that.

But it really depends on the case, the spread of the case, how far it takes you, whether or not if you are operating in Turkey or Morocco or Estonia or Latvia or Romania or France, England, Sweden, something like that, it brings in the legal attache’s office, and our people spend a fair amount of time coordinating with their counterparts overseas. I did not just mean Europe, but also in the Far East, quite obviously.

And so it can take a lot, but you take down something like Coreflood, and with the innovative ways of addressing that, it was a relatively small group of people in New Haven and headquarters and some across the country and some internationally that were able to undertake that. And once you develop, as you would know as a prosecutor, a template for doing these kinds of cases, it is easier the next time around.

Senator WHITEHOUSE. Easier the next time. Very good. I see that Senator Coons has returned from the vote that is going on right now on the Senate floor, and I recognize him.

Senator COONS. Thank you, Senator Whitehouse. The Senate is voting now on an amendment to the United States Constitution, and our Chairman is about to speak, so please forgive the interruption, if you would, in this hearing.

Director Mueller, thank you for your service and for your testimony here today and for your willingness to continue in a leadership role at the FBI. As you were just discussing with Senator Whitehouse, one of the challenges, I think, that we face in this particularly difficult budgetary environment for State and local law enforcement around the country is the steady downward pressure on local law enforcement agency budgets.

In my role as county executive before becoming a Senator, one of the things we relied heavily on was an effective partnership with the FBI. The FBI works very well and closely with State and local law enforcement through a task force structure and does a lot of information sharing.

Talk, if you would, a little bit about how the FBI and DOJ have institutionalized openness and partnering with local law enforcement through the National Data Exchange, or N-DEX, and others, and what impact you have seen on the reach and effectiveness of your multi-agency task forces given what I presume must be the

steadily decreasing availability of local law enforcement partners given the budgetary pressures local law enforcement currently face.

Mr. MUELLER. Let me start by saying my belief is that we are most effective when we work in task force, or work in joint investigations. Bringing together expertise from a variety of different places enhances your capability. I worked here in the U.S. Attorney's Office, and they had a cold case squad with FBI agents working with homicide detectives from the Metropolitan Police Department, and the homicide detectives were some of the best investigators I have ever seen. The FBI brought capabilities that State and local did not have, and it worked exceptionally well. And that in my mind has been a model.

Out of that has come, as I think I have said in some of my remarks, over 150 State and local task forces relating to violent crime and drugs and gangs in particular. We had, I think, 34 or 35 Joint Terrorism Task Forces in 2001. We are now up at around 100. We have Safe Trails Task Forces in Indian country, and we now around the country have started Cyber Task Forces. We have regional forensics labs which relate to the handling of cyber material and the forensics aspect of it. And so we have developed these over a substantial period of time.

When it comes to cyber in particular, we are at the threshold of a development of an approach to cyber crime across the country, and I say that because in the past the State and local law enforcement have not been able to develop the capabilities in this arena as far as perhaps we have and look to us, look to the Secret Service and look to others to handle much of the more important work. The impact of the cyber arena is such that in the future the Federal authorities will not be able to do it alone, and we are going to have to continue to develop the task force structure and have State and local law enforcement develop the capabilities to address cyber in the same way that State and local law enforcement has developed it in a variety of areas in the past.

I will tell you that when I visit offices, when we have them and have an exchange about what is happening in particular offices around the country, one question we ask is: Have you seen State and local law enforcement officers leaving task forces because of the budget constraint? And very rarely is that happening. I do believe that State and local law enforcement appreciate the opportunity to participate at that level and find that participating in these task forces leverages their capabilities, and it is not just having a person on a task force, but they can be more effective as a State and local department with having persons on the task force.

Senator COONS. Well, that is a testament to the value that State and local law enforcement finds in partnering with the FBI because of your superior intelligence and specialized unit capabilities and your National information-sharing role. You referred to cyber crime, something we are both very concerned about, as are a number of my colleagues. There have been a number of recent reports suggesting that cyber crime has exploded in the last decade, that it is growing at a dramatic pace, that it has consequences not just for individuals and for harm to them, but also broader harm to our economy. In fact, I think it was the Executive Assistant Director for the FBI that described it as an "existential threat" to the

United States. And I am wondering—I know you and Senator Whitehouse just had an exchange about this—whether you are resourced effectively in terms of the number of agents, the training. I know you have very difficult choices to make, many different areas of challenge in your service.

If I understand right, there are about 1,000 advanced cyber-trained FBI agents, but nearly five times that many dedicated to the war on drugs. There have been some studies that have suggested that at the State and local level we do not have enough professionals, law enforcement officers trained to the right level.

How do you feel we are doing at staffing and training in the FBI to meet the level of threat? And what else could we in the Congress be doing to support you in that effort?

Mr. MUELLER. In the wake of September 11th, we knew we had to prioritize and in the wake of September 11th move 2,000 agents from the criminal side of the house to national security, particularly counterterrorism. Of those, approximately 1,500 were in the drug program. Another 500 were doing smaller white-collar criminal cases, but we had to prioritize.

We have doubled the number of agents—almost doubled the number of agents that are doing cyber work at this juncture, and we have a number of specialists in addition to agents who do the forensics and work on it.

Our drug cases are in the context of OCDETF and the joint task force arena. We rarely at this point in time do any individual drug cases such as we did beforehand.

Do we need additional resources? Yes. Is the No. 1 request I make each year in the last several years when we took care of counterterrorism to a certain extent a request for more agents in this arena? It is. Has Congress given us some? Yes. In any one of these, is it enough? Probably not. Part of it is also our prioritize, our reorganization so that we can address these cases more efficiently, and it goes to something I was saying to Senator Whitehouse, and that is, around the country we will have this area of expertise, and where in the past it was important to have it localized on local cases, that expertise has to be utilized to address cyber cases wherever they may arise because often at the outset of any intrusion you do not know where the home is. And, consequently, we as an organization have to adapt as well as getting additional resources, but adapt our structure and our organization to be more efficient in handling these cases.

Senator COONS. How does the FBI differentiate between a criminal cyber threat and one that implicates the national security and that then implicates other non-law enforcement but more military-oriented assets in the cyber field?

Mr. MUELLER. Well, we established a National Cyber Investigative Joint Task Force. It might be worthwhile for you to visit it if you have not. But it has ourselves and other relevant agencies in this arena, intelligence agencies as well as law enforcement agencies. And so in conjunction with NSA, for instance, and others, once a substantial intrusion is identified, it will be looked at, and the beginning work forensically will be done by a number of contributing agencies who have that expertise without putting it into a particular cubbyhole at the outset. You do not know whether the

person is a foreign state or an organized crime group or an organized crime group operating at the behest of a state or the high school student in a bedroom down the block.

And so we treat them each at the outset with the same approach to dissect it and try to identify it, and once you get an identification you can make a decision, OK, this is domestic, it is a criminal case, it will be handled domestically, or no, it is a national security threat that ought to be handled by our military in some way, shape, or form, and then allocate—or then tag it with, OK, how are you going to resolve this, how are you going to disrupt this threat.

Senator COONS. And that exact process, that interface, that decisional iterative process is of great interest and concern to me given your exchange with Senator Sessions and Senator Feinstein previously in the context where in the National Defense Authorization Act a number of us have raised real concerns about the possibility of uncertainty. I would agree with you. I take very seriously your written input to the Senate that you have real concerns about the possibility in the short run and the long run that the military and law enforcement will begin having an unresolved and unclear joint role in investigations, in apprehension, in the early stages of trying to encourage cooperation and that in the lack of a resolution there, there is both a threat to civil liberties and a possibility of missing vital opportunities for us to advance our National security.

In the national security context, in the counterterrorism context, it implicates constitutional liberties, civil liberties, and our National security, and I think that is true both in cyber and in the development at the very earliest stages of potential counterterrorism cases within the United States.

Speak, if you would, about how you would encourage us to resolve some of these longer-term issues. There was no specific hearing for the detention provisions of the NDAA. There were a number of us who voted to pull those provisions out of the Defense Authorization Act to have a brief period where we would have focused hearings, get input, but it concerned me deeply that leaders in our law enforcement and counterterrorism and national security communities in the current administration opposed the language in that bill. And without having the benefit of a hearing or full development of this intersection between security and liberty, I was gravely concerned about our moving forward with this language.

How would you advise us to deal with this in a way that does not deprive law enforcement of critical tools in the fight against both cyber crime and terror?

Mr. MUELLER. Well, I would hesitate to try to advise Congress in this way. What I tried to do is express the concerns I have with the language that has been presented, and, again, it focuses on—part of it has been resolved in terms of our ongoing authorities, for which I am grateful. The other level of concern relates to the uncertainty of what is going to happen at the time of arrest and what is going to happen in terms of investigations down the road. Is it going to go military? Is it going to go Article III? And the statute is still unclear in terms of allocating that.

Now, I know the argument on the other side is that will be cleared up by procedures, and that will be developed by the President, and the President has the waiver authority. Given the statute

the way it is now, it does not give me a clear path to certainty as to what is going to happen when arrests are made in a particular case and the facts are gray, as they often are at that point, and the possibility looms of we will lose opportunities to obtain cooperation from the persons that in the past we have been fairly successful in gaining.

Senator COONS. Well, I see that it is time for me to conclude my questions. I just want to congratulate you and the agency for being a very successful partner in the war on terror and in the effort to isolate, identify, and prosecute folks who are engaged in domestic efforts at terrorism. I want to thank you for your efforts in combating cyber crime, and in particular some of the issues that Senator Kohl raised about trade secret theft are a real interest and concern to me, and I would like to note I share Senator Franken's concerns about some of the as yet unknown privacy implications of the software on our cell phones.

Thank you very much for your testimony today.

Thank you, Mr. Chairman.

Mr. MUELLER. Thank you.

Chairman LEAHY. [Presiding.] Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman, and thank you, Director, for your public service not only in your present role but throughout your career as a prosecutor and as a member of our military, and thank you for being so forthright in your answers today to some difficult areas of questioning.

I want to come back to cyber but in a different context, and I am very concerned about cyber attacks on this country, which General Petraeus has said will be our next 9/11, and you have very vividly and graphically described what you view as the threat. But the threat to women and children on the Internet I think is equally troubling, and I proposed a bill called the Internet Abuse Act, which would be a companion to the reauthorization of the Violence Against Women Act, which focuses on stalking, intimidation, harassment, which can lead to physical violence when it occurs on the Internet, lead to physical violence then in the real world.

I would like to get from you some sense of what you view as the perils and the dangers on the Internet to children and women and what the FBI is doing to combat them.

Mr. MUELLER. Well, we have a number of programs to address that. Our one program we have had for years is the Innocent Images program that I think you are probably familiar with from your time as Attorney General in Connecticut, in which we operate undercover on the Internet to identify stalkers, and particularly it is related to children.

The threat that you articulate to women and children on the Internet is growing daily, and the ubiquitous nature of the Internet is such that it is very difficult to address and to educate persons because a number of people, including occasionally myself, are baffled by what happens when certain things—when you are on the Internet and getting on the Internet, many people I think are baffled by the privacy protocols and uncertain as to how to utilize them. But our programs are directed at identifying those persons who are luring children into sexual liaisons on the Internet. Quite obviously, beyond that there are and have been prosecutions, most

recently I think in California, for persons who were stalking in some sense on the Internet, but also others who were driving—particularly in schools, driving other children to suicide and the like. And so the variety of harm that can come from abuse on the Internet is substantial.

We have throughout the country over the last several years put together with U.S. Attorney's Offices, FBI, as well as State and locals ICAC teams that address this together, but there is so much of it out there you have to prioritize. And, again, it is going to be—I absolutely agree that it is going to be a huge issue in the future, this particular area, and anything that can be done legislatively to enhance the penalties, enhance the certitude of conviction appropriately, and deter persons from abuse on the Internet will be welcomed.

Senator BLUMENTHAL. Well, I am glad to hear you make that comment because that is exactly the goal of the measure that I proposed, to enhance the certitude and make penalties more severe so that individuals who, in effect, are aiding and abetting or enticing or luring or harassing on the Internet can be held more accountable. And I am delighted to hear that you would consider supporting that kind of measure.

I also want to ask you, if I may, about human trafficking by Federal contractors abroad. You may be familiar with this problem where contractors on our bases abroad in effect take advantage of individuals who are recruited from Third World countries, more than 100,000 foreign nationals working on our bases abroad, sometimes exploited by our contractors. And, again, I have worked with the Chairman—and I thank Senator Leahy for his support—to try to target and criminalize the human trafficking of persons working for contractors abroad under conditions and terms that would not be tolerated in this country. And I would like to ask you whether the FBI is doing anything on the enforcement side with respect to this problem.

Mr. MUELLER. This is an issue that I am not familiar with. I will go back and see what, if anything, we are doing in that arena. Since our presence usually is in embassies, not really on military bases, that falls to the various law enforcement entities in the military generally. But I will go back and see what, if anything, we are doing here, and if there is any issue with regard to our jurisdiction to investigate or prosecute in an Article III court, we will get back to you on that.

Senator BLUMENTHAL. I appreciate that. And, finally, because my time is almost up, you mentioned the idea in your responses to one of the questions, perhaps from Chairman Leahy, of making a cyber crime a predicate under the Racketeering Act. I wonder if you could expand on that thought.

Mr. MUELLER. Only to say I think it is a good idea, that it would enhance—it should be a predicate, in my mind, and the sentences attendant to a conviction on racketeering are substantial and would send the message.

I think too often in the past we have looked at individuals who were involved in cyber crimes, and they may be relatively young individuals, and there may be a perception among some that it is a turnstile. Yes, you may get caught, yes, you may be convicted,

but you will be walking out relatively soon, and the crime may be worth the time that you spend. That cannot be the message that is sent. The message to be sent is that if you engage in cyber crime you will go to jail, and you will go to jail for a substantial period of time.

Senator BLUMENTHAL. And I think that observation, your support for that kind of measure, illustrates the kind of gaps that may be arising. The Internet Abuse Act that I proposed is one measure trying to address them, but using a cyber act, so to speak, as a predicate for a racketeering violation I think is a very promising avenue that we should explore. Thank you.

Mr. MUELLER. Thank you.

Chairman LEAHY. Thank you very much, Senator Blumenthal.

Senator Klobuchar.

Senator KLOBUCHAR. Well, thank you very much, Mr. Chairman. Thank you also, Director Mueller, for being willing to stay through our votes and everything else and for your good work. You have served the FBI so admirably. I think it is quite a testament that President Obama asked you stay for another 2 years, and you were confirmed by a vote of 100–0. That is usually like for volley ball team resolutions or something, so excellent work.

I wanted to ask about something that has been on my mind because this Committee passed the synthetic drug bill. I have one, Senator Schumer has one, Senator Grassley has one. The one I have deals with a synthetic hallucinogen known as 2C-E. As you probably know, the House passed similar versions of these bills this past week. In our case in Minnesota, this young man died and the problem, as you know, is nationwide. I just think it is incredible, talking to some of our police chiefs, especially in the rural areas of our State, where they have seen this increase in these cases, and it is very difficult if you are in a city like Moorhead as opposed to Minneapolis to try to get experts to prove what the substance was. And in the first half of 2011, there were roughly 6,600 calls to poison control centers across the country. That is 10 times the amount we had in all of 2010. So it is clearly a growing issue.

Senator Paul currently has a hold on these bills in the Senate. We are trying to get them done by the end of the year. I had a good talk with him yesterday. I hope we will be able to work this out. But I wanted to get your take on this problem. One of my views is we can add these substances to the schedule, but we still have an issue with the way the analog statute works that we may want to make some amendments going forward. That is something I want to work on, but let me get your take.

Mr. MUELLER. I am afraid I cannot be as much help as perhaps I would want to be because it really falls within the purview of my friends at the DEA, what you are getting at. But to the extent that it is coming along in the same way that OxyContin or some of the other drugs, we have to watch it, and together with State and locals and our friends at DEA, not only would we want to watch it, but also have the statutes in place that enable us to appropriately address it and send the persons who were involved in this kind of trafficking to jail.

Senator KLOBUCHAR. Very good. Well, we have been working with DEA, obviously, and they came out and did—along with Gil

Kerlikowske, and we have been working on it. But I just want to call it to your attention.

I also know that the FBI and the DOJ have been focusing on the health care fraud issue.

Mr. MUELLER. Yes.

Senator KLOBUCHAR. Minnesota tends to have better enforcement in those areas, and I know there are certain areas known as “hot spots” where a lot of our health care dollars are getting sucked down to places that are not as good at trying to track these things. Could you talk about those efforts and what you have seen with the coordination with the HEAT task forces.

Mr. MUELLER. One of the interesting things is the benefit from building an intelligence capacity to address counterterrorism and then bringing it to bear in the criminal arena. We have found, as you point out, that there are health care hot spots where there will be schemes and plots that are utilized for a period of time by a number of individuals. There will be an enforcement effort that shuts it down, often by a task force of ourselves working with individuals who are from the AG’s office or from State and local, but then it will pop up someplace else.

One of the things the building of an intelligence infrastructure across the country enables us to do is to identify this, educate others, and be on the alert for other places where the same hot spots may grow if we do not get in there early and address it. And so with a combination of task forces, identification of those, as you call them, hot spots where the activity is particularly high, but also with the use of intelligence to identify where the persons are going to move next, we have had some impact.

It is still billions of dollars. It is still rampant out there. But we have increased personnel, and we have identified and added persons across the board to address health care. And I think we are being effective, but there is still more work to be done.

Senator KLOBUCHAR. Very good. I know you talked to some of my colleagues about cybersecurity. Actually, one of the examples that you used was Cargill—Cargill is based in Minnesota—in your testimony of some stolen secrets that they experienced.

Mr. MUELLER. Yes.

Senator KLOBUCHAR. And I just see this as the next big thing we need to work on, cybersecurity for our country, but also Internet fraud and some of the things that we are seeing being stolen. The Internet Crime Complaint Center, or IC3, is a partnership, as you know, with the FBI and the National White-Collar Crime Center aimed at addressing Internet crime.

In my former job as a prosecutor, this was just at the beginning of all this, and we would have local police who would be confronted with computers, and they would turn them on, and everything would vanish. We have gotten much better than that, but there is so much of an issue for local police not having the resources to deal with this, so much of it international.

Could you give us an update on that? And where do you think we need to go?

Mr. MUELLER. Well, we have to build our resources across the Government and better organize to address cyber, identify the lanes in the road with some additional particularity. At home we

have to adjust our organizational structure to address cyber. One of the points I do make is we have expertise around the country, but you never know where an intrusion is going to arise, much less from whence it came. And, consequently, we as an organization have to address cyber crime differently than we address bank robberies, which was localized and the expertise was across the country. Here we do have expertise across the country, but often the crime can shift from city to city, county to county, country to country, and we have to be able to address that, and that is what we are working on.

I will say that today, of the number of Senators who have questioned me—maybe six, seven, eight—maybe four of them have been focused on cyber crime. Four years ago, one would not have. And I venture to say when we meet again, as undoubtedly we will next spring, that it will be a No. 1 issue on the agenda. Too often, in a variety of ways, the statutes do not keep up with technology, particularly in this day and age and, consequently, the work of this Committee to provide the tools to address the enhanced technology will be tremendously important.

Senator KLOBUCHAR. Well, thank you very much for that. We look forward to working with you.

Mr. MUELLER. Thank you.

Senator KLOBUCHAR. Thank you.

Chairman LEAHY. I will put in the record or submit to you for answers some questions by Senator Grassley, and if I have other questions, I will submit them for the record.

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

Chairman LEAHY. Not seeing others and knowing what is going on on the floor, we will stand in recess, but with the appreciation of the Committee to Director Mueller.

Mr. MUELLER. Thank you, sir.

[Whereupon, at 12:05 p.m., the Committee was adjourned.]

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

QUESTIONS AND ANSWERS



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 15, 2012

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 December 14, 2011.

We sincerely 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,

A handwritten signature in black ink, appearing to read "R. Weich".

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 December 14, 2011, Hearing Before the
Senate Committee on the Judiciary
Regarding "Oversight of the FBI"**

Questions Posed by Senator Feinstein

1. Has ICANN been effective in preventing Internet domains from being used for criminal activity in the current domain environment?

Response:

ICANN's mission of coordinating the technical management of the Internet domain name system (DNS), including its contractual agreements with accredited Registrars and Registries, provides a platform to address law enforcement concerns regarding criminal activity using domain names. In response to a direct request from ICANN's Governmental Advisory Committee (GAC) in October 2011, the ICANN Board directed ICANN staff to initiate negotiations with Registrars to develop amendments to the Registrar Accreditation Agreement (RAA) consistent with recommendations proposed by international law enforcement and endorsed by the GAC. These negotiations are underway and are being closely monitored by the USG. ICANN needs to move swiftly if it is to effectively provide tools for law enforcement to combat the criminality surrounding domain names. In addition, ICANN needs to address apparent deficiencies in the implementation of WHOIS policy, including the need to authenticate WHOIS entries. The U.S. Government strongly supports a majority of the recommendations of the Affirmation of Commitments WHOIS Review Team in this area and expects the ICANN Board will take appropriate action on them at its June 2012 meeting. The USG has also advanced a consensus GAC position that has been formally transmitted to the ICANN Board that ICANN's contract compliance function must be improved to ensure that Registrars and Registries fully implement the provisions in their respective agreements with ICANN that address law enforcement concerns.

2. I understand that many concerns regarding Internet criminal activity stem from a failure of Internet registries and registrars to abide by their contractual obligations with ICANN. Can you suggest any methods that ICANN could use to improve its registry and registrar contractual compliance?

Response:

These responses are current as of 2/24/12

As noted above, negotiations are currently underway that the USG expects to strengthen the Registrar Accreditation Agreement (RAA), the contract between ICANN and its accredited registrars, based on the proposals of law enforcement agencies as endorsed by ICANN's Governmental Advisory Committee (GAC). U.S. law enforcement agencies were instrumental in developing these recommendations and securing GAC endorsement of them. Key provisions include collecting and verifying accurate and truthful registrant information, maintaining public and accurate WHOIS records, requiring all registrars and registries to have transparent business disclosures, publically displayed "point of contact" (POC) information (including addresses), and specific POCs for reporting abuse, and introducing more clear and consistent requirements for the provision of privacy and proxy services, which permit domain name registrants to shield their identities. Data from FBI field offices indicates that such services are used by some domain name registrants to engage in criminal activity. Updating the RAA and further funding and staffing ICANN's contract compliance function will help ICANN more effectively enforce the relevant provisions in its contracts with accredited Registrars and Registries.

3. Are there structural or organizational benefits or impediments to members of the international law enforcement community providing concerns to ICANN? Are there any structural or organizational benefits or impediments to members of the international law enforcement community implementing solutions to any concerns raised?

Response:

ICANN's multistakeholder structure provides representational opportunities for a diverse and broad range of interests, including governments. One of ICANN's advisory committees is the Governmental Advisory Committee (GAC), which is composed of representatives from over 100 national governments. The U.S. is represented in the GAC by the National Telecommunications and Information Administration (NTIA) which convenes a monthly USG DNS issues interagency meeting to develop coordinated USG positions and strategies. This process has enabled the U.S. representative to be a strong advocate for law enforcement interests and effectively raise them in the multistakeholder process. However, due to historical structural impediments, it has been a challenge to have these positions and strategies fully addressed.

4. As we discussed at the hearing, ICANN has developed a new Generic Top-Level Domains (gTLD) program. How does law enforcement view this process? May it be a benefit or a threat to preventing online crime?

Response:

USG positions for the GAC are coordinated with all federal agencies, including law enforcement, through a monthly DNS issues interagency group. This was the case with

These responses are current as of 2/24/12

respect to the new gTLD program where U.S. Government recommendations related to law enforcement were based on input from Federal Bureau of Investigation (FBI), the Food and Drug Administration (FDA), the Drug Enforcement Administration (DEA), and the Federal Trade Commission (FTC). All of the USG's submissions to the GAC on these issues were endorsed and formally included in the GAC Scorecard and the U.S. served as the GAC lead on these issues during the exchanges between the GAC and the ICANN Board. All of the GAC recommendations related to law enforcement and consumer protection identified in the Scorecard were adopted by the ICANN Board. While there are some up-front protections embedded in the new gTLD applicant evaluation process that are intended to minimize the potential that a criminal enterprise or an entity either investigated for or charged with criminal activity could become a new gTLD registry operator, the potential for abuse and fraud remain. The GAC Law Enforcement recommendations are designed to address many aspects of this potential.

5. It has come to the attention of my office that members of law enforcement have made recommendations to ICANN in its new gTLD proceeding to prevent use of new Internet domains for criminal activity. Do you know what those recommendations were? How many of those recommendations have been accepted by ICANN? How critical are those recommendations that were not accepted?

Response:

At the 2009 ICANN meeting in South Korea, law enforcement "Due Diligence Recommendations for ICANN" were formally presented to ICANN through the GAC, with the GAC formally endorsing and forwarding to the ICANN Board, those twelve recommendations at the ICANN meeting in Brussels in 2010. Those recommendations were a collaborative effort by the FBI, U.S. Department of Justice (DOJ), United Kingdom Serious Organised Crime Agency, Australian Federal Police, Royal Canadian Mounted Police, and New Zealand Police to aid in the "prevention and disruption of efforts to exploit the domain name registration by Criminal Groups for criminal purposes." The recommendations were drafted to aid law enforcement in tracing criminals who use domain names to further their criminal ventures.

To date, ICANN has accepted and implemented only one of the recommendations. The one recommendation implemented by ICANN is II(a): "ICANN [is] to conduct enhanced due diligence on all Registrars and Registries (including but not limited to owners, officers, board of directors) ICANN accredits, or has accredited. . . ." While ICANN has not acted on any of the other law enforcement recommendations, they are being considered as part of the current RAA negotiations.

6. It is also my understanding that U.S. law enforcement has coordinated with other members of the law enforcement community internationally to develop the new gTLD

These responses are current as of 2/24/12

recommendation. Could you please list the members of the international law enforcement community who agree with the recommendations?

Response:

As noted above, these law enforcement recommendations were developed by the GAC, which is composed of representatives of numerous national governments. The development of the recommendations was a collaborative effort by the FBI, DOJ, United Kingdom Serious Organised Crime Agency, Australian Federal Police, Royal Canadian Mounted Police, and New Zealand Police.

In its work with ICANN to stem criminal activity related to the DNS, the FBI has coordinated and collaborated with numerous domestic and international law enforcement partners. Following are the law enforcement organizations with which the FBI has worked the most closely.

- G-8 Lyon-Roma Group / High Tech Crime Subgroup (Germany, Canada, United Kingdom, United States, Italy, Japan, and Russia)
- Interpol – Interpol Working Party on IT Crime - Europe
- Australia – Australian Federal Police
- Brazil – Brazilian Federal Police
- Canada
 - Royal Canadian Mounted Police
 - Quebec Provincial Police
- New Zealand – New Zealand Federal Police
- South Korea – South Korean National Police
- Spain – Guardia Civil
- Switzerland – Federal Department of Justice and Police
- Thailand – Ministry of Justice
- United Kingdom
 - Serious Organized Crime Agency
 - Metropolitan Police
- USA
 - Immigration and Customs Enforcement (Homeland Security Investigations)
 - Drug Enforcement Administration
 - Federal Trade Commission
 - Food and Drug Administration

These responses are current as of 2/24/12

Questions Posed by Senator Schumer

Increased Shootings of Law Enforcement Officers

7. Director Mueller, in the past week, we've tragically witnessed several high profile shootings of policemen, including one in New York City. We lost a brave police officer Peter Figoski—who was responding to a home invasion in Brooklyn. According to initial reports, his murderer committed the crime with an illegally purchased gun and should have been locked up weeks ago for shooting a man in North Carolina.

... **According to the National Law Enforcement Officers Memorial Fund, there were 4 other police officers shot and killed last week too (including at Virginia Tech University). And by their analysis, firearms-related police fatalities are up nearly 20% this year – and that follows on a significant increase in 2010 as well. We've also seen U.S. Marshals killed this year in Florida, Missouri, and West Virginia.**

a. Is the FBI keeping track of whether the murderers in these cases were prohibited purchasers?

b. Similarly, is the FBI keeping track of whether these murderers went through a background check for the weapons they used to kill police officers? If not, why not?

Response to subparts a and b:

When a National Instant Criminal Background Check System (NICS) check is requested, applicable regulations (28 C.F.R. § 25.9) require the FBI to destroy transaction content containing the personally identifiable information of a firearm transferee within 24 hours of informing the Federal Firearms Licensee that the transaction may proceed. Even though a transaction “may” proceed, the transaction does not always take place, and the FBI has no way of knowing when or whether a given transaction has, in fact, occurred. The FBI is also not permitted to record the serial number or other details describing the firearm involved, so we are not able to later determine whether that weapon was used to kill a police officer.

The FBI is, though, permitted to retain records indicating a denied firearm purchase. We have determined the neither Lamont Pride (suspected in the death of Officer Figoski) nor Ross Truett Ashley (suspected in the death of Virginia Tech University Officer Deriek Crouse) were denied firearm purchases based on NICS checks.

These responses are current as of 2/24/12

8. Why do you think we're seeing an increase in law enforcement shootings? And what can be done with new technology to help prevent these horrific incidents from occurring in the future.

Response:

The information maintained by the FBI's Uniform Crime Reporting Program includes statistics related to Law Enforcement Officers Killed and Assaulted (LEOKA). The LEOKA statistics maintained over the past decade reveal an increase in the number of unprovoked attacks on law enforcement officers. The FBI is interviewing convicted offenders who have participated in these events to better understand the events and those involved. We look forward to sharing with the law enforcement community any information obtained through this process that will help to improve their safety.

In addition, in order to improve the ability of law enforcement officers to survive these assaults, the FBI provides to law enforcement officials Officer Safety/Awareness Training that emphasizes officer awareness and other techniques designed to mentally prepare the officer to survive a potentially deadly encounter. This training is provided to federal, state, and local law enforcement agencies free of charge.

Utica College

9. As you may know, cybercriminals, whether a criminal hacker, a foreign agent, or a terrorist, are a growing threat to the safety and security of all Americans. This past June I sent you a letter urging the FBI to utilize Utica College's Cybersecurity Training center, a state-of-the-art cyber security intelligence program and forensic training center, to train special agents in the most advance techniques for preventing and protecting against cybercrime. I want to once again urge you to work Utica College to form a partnership aimed at strengthening the capabilities of the FBI cybercrime division.

a. Would you agree to look into starting such a relationship?

b. Do you pledge to visit yourself or send a high ranking official from the FBI to visit Utica College's Cybersecurity Training Center?

Response to subparts a and b:

We agree with Senator Schumer that cyber crime is a growing threat to our safety. As acknowledged in the FBI's responses to both Senator Schumer's June 2011 letter and a June 4, 2011, letter from Utica College, investigating cyber crime presents significant and unique challenges and the FBI is always evaluating ways to provide cyber education for our employees through traditional classrooms and virtual teaching environments. We

These responses are current as of 2/24/12

recognize the value of joint cyber security collaborations with colleges and universities and we appreciate the effort to bring Utica College's programs and resources to our attention. We will continue to assess the possibilities afforded by our colleges and universities along with any procedural requirements or restrictions placed on our entry into contractual relationships in this context.

Questions Posed by Senator Franken

10. Has the FBI ever received, requested, requested access to or accessed any information from Carrier IQ, whether or not it was produced by their software or as a result of a business meeting between the FBI and Carrier IQ?

Response:

The FBI routinely communicates with numerous technology companies relative to new and emerging technologies. A review of our records indicates that the FBI has not served legal process (such as a search warrant) on Carrier IQ to obtain subscriber data and has not directly received, requested access to, or knowingly accessed information from Carrier IQ in support of an ongoing investigation.

11. Has the FBI ever received, requested, requested access to or accessed any information from any wireless carrier that was generated by Carrier IQ software?

Response:

When the FBI serves legal process on a wireless carrier seeking subscriber information, the wireless carrier does not disclose the origin of the data. Since the wireless carrier does not attribute the source of the information provided to law enforcement, we cannot determine whether the information was generated by the wireless carrier's own network infrastructure or by a third party vendor supporting the wireless carrier.

Questions Posed by Senator Grassley

Office of Legal Counsel Opinion on Anwar al-Awlaki

These responses are current as of 2/24/12

12. On September 30, 2011, it was reported that Anwar al-Awlaki, a U.S. citizen, was killed in an operation conducted by the United States in Yemen. According to media accounts, the operation was conducted following the issuance of a secret memorandum issued by the Department of Justice authorizing the targeted killing of a U.S. citizen abroad. The published accounts include details provided by “administration officials” and describe the memorandum as the product of a review of legal issues raised by targeting and killing a U.S. citizen.

I, along with Chairman Leahy, have requested a copy of this memorandum from the Justice Department. Despite the Administration publicly acknowledging the memorandum’s existence to the media, it has not yet been provided to Congress. At the hearing, I asked you about this letter and whether you supported Congress having access to it. You replied that it was not your role in determining whether Congress should have access.

a. Do you agree that Congress has an obligation to conduct oversight of the targeted killing of an American citizen by the United States?

Response:

The FBI’s authorities and responsibilities, which are established by statute, do not include determining Congress’ obligations.

b. Do you agree that, to the extent practicable, decisions as important as the legal authority granting the Government permission to kill an American citizen should be made public? If not, why not?

Response:

We defer to others in the Administration for response to this inquiry.

Anthrax Leak Investigations

13. The Anthrax investigation spurned an unfortunate situation where someone in the Justice Department leaked sensitive information regarding the investigation to the press. Those leaks involved alerting the media that Dr. Steven Hatfill was under investigation and that search warrants were going to be executed on his residence. Ultimately, Dr. Hatfill was exonerated of any wrongdoing in the case, and the Department of Justice settled a civil lawsuit filed by Dr. Hatfill based upon the Department’s violation of the Privacy Act. This settlement cost the American taxpayers nearly \$6 million and occurred based upon the Department’s leak of information to the press.

These responses are current as of 2/24/12

I wrote to you on August 31, 2011, asking you for a status update on the investigation into the leaks at the Justice Department related to Dr. Hatfill. In response to my letter, the Justice Department stated, "After an extensive investigation, career prosecutors concluded that, based upon the Principles of Federal Prosecution, criminal charges were not appropriate in this matter." However, there was no further information provided.

At the hearing, I asked you three questions, (1) Were the individuals who leaked sensitive information regarding the investigation of Dr. Steven Hatfill FBI agents or employees of the FBI? (2) What, if any, administrative action did you take against these individuals if they were FBI agents or employees? (3) And, do these people still have their jobs if they're FBI employees? You responded that these questions "are more specific than the ones you raised when we met. I would have to get back to you on it because it is specific to the FBI. I know there were other entities other – entities than the FBI and the Department of Justice that have undertaken an investigation as well. So I will have to get back to you on that." Given no criminal prosecution occurred, I want to know if any action was taken against the leakers given they must have been identified if criminal prosecution was considered and declined.

a. Were the individuals who leaked sensitive information regarding the investigation of Dr. Steven Hatfill FBI agents or employees of the FBI? If yes, please provide the names, titles of the individuals, and their pay grades.

b. If they were not FBI employees, what federal agency were they employed by? If they are Department of Justice personnel, provide the names, job titles and pay grades of those individuals.

c. What, if any, administrative action did you, or the Attorney General, take against these individuals if they were FBI agents or employees?

d. Do these individuals still have their jobs?

e. What is the FBI's official policy on leaking the names of individuals subject to investigation?

f. Did the leak investigation identify whether any rule, regulation, or policy at the FBI or Justice Department was violated? If so, please provide a copy of the rule, regulation, or policy related to leaking investigative information to the press.

Response to subparts a through f:

These responses are current as of 2/24/12

Dr. Hatfill's constitutional rights and privacy protections were the subject of litigation against DOJ, the FBI, and others, which was settled in 2008. Among other things, Dr. Hatfill's complaint in that case addressed then Attorney General Ashcroft's identification of Dr. Hatfill as a "person of interest" in 2002. It is the FBI's understanding that DOJ's Office of Professional Responsibility (OPR) investigated the leak of law enforcement sensitive information regarding the anthrax investigation. The FBI defers to DOJ's OPR regarding the results of that investigation.

In addition to the Privacy Act and the Freedom of Information Act, there are both DOJ regulations (see, for example, 28 C.F.R. § 50.2, "Release of information by personnel of the Department of Justice relating to criminal and civil proceedings") and FBI policy (for example, on the FBI's Internet website, www.fbi.gov, use the "Search" window to locate the Frequently Asked Question: "Can I obtain detailed information about a current FBI investigation that I see in the news?") addressing the disclosure of information regarding criminal investigations. When release is permitted by law, both DOJ and FBI policy recognize that there are circumstances in which the public disclosure of investigative information is appropriate. For example, the rationale behind the publication of the FBI's "Ten Most Wanted Fugitives" and "Most Wanted Terrorists" is that, if the public has information regarding wanted fugitives and terrorists, they can assist the FBI in identifying and arresting these individuals.

FBI Whistleblower Jane Turner:

14. Agent Jane Turner filed a whistleblower complaint with the Department of Justice, Office of the Inspector General (OIG), in 2002 when she discovered that FBI agents removed items from Ground Zero following the terrorist attacks of 9/11. Unfortunately, Agent Turner was forced to file an appeal to the Office of Attorney Recruitment and Management (OARM) due to the OIG's delayed decision in their investigation. Ultimately, the OARM substantiated her allegations in May, 2010, and the FBI was ordered to provide Agent Turner back pay, attorney's fees, and other relief. The FBI has filed an appeal to the Deputy Attorney General concerning the issue of back pay, despite the FBI's failure to raise the issue of back pay during previous OARM proceedings. The case was remanded back to OARM for further investigation, and a final resolution to Jane Turner's reprisal case against the FBI is now further delayed. Agent Turner initially filed her complaint approximately 9 years ago, and she has yet to receive a final decision.

a. Why has the FBI continued to appeal Ms. Turner's case to the Deputy Attorney General despite a decision by OARM?

b. You have repeatedly stated you will not tolerate retaliation against whistleblowers at the FBI, yet the FBI continues to appeal Ms. Turner's case—losing both in Federal Court and at the OARM. Do you believe continuing to appeal this case, 9 years

These responses are current as of 2/24/12

after it was filed, sends a message to whistleblowers that their concerns will be taken seriously by FBI management? If so, please explain why. If not, why continue to appeal her case?

c. To date, how much has Ms. Turner's case cost the FBI? This includes defending her suit in district court, the OARM proceeding, and appeal and briefs to the Deputy Attorney General?

Response to subparts a through c:

The Director of the FBI works hard to make clear to all FBI employees that whistleblower retaliation will not be tolerated. While the FBI does not accept the factual assertions in the question, we believe the most important point is that we do not see participation in the legal system as contradicting the Director's commitment to whistleblower protections. Instead, we believe it sends a consistent message that it is important to honor the law, regardless of what interests the law is perceived as protecting. The purpose of the legal system is to protect all parties, not just whistleblowers or their supervisors, not just employees or employers.

Just as Ms. Turner has sought review of numerous decisions, the FBI appealed the decision of DOJ's Office of Attorney Recruitment and Management (OARM) to the Deputy Attorney General, as permitted by the governing regulations, on the grounds that it was "not in accordance with law" and was "unsupported by substantial evidence." The Deputy Attorney General remanded the issue of back pay relief to OARM, which obtained briefs from the parties before rendering a new decision that was consistent with the precedent established by Federal Circuit court cases. Ms. Turner has now appealed OARM's decision to the Deputy Attorney General, as she is entitled to do.

The FBI does not maintain records reflecting the amount of time spent by FBI attorneys on individual cases.

FBI Whistleblower Robert Kobus

15. Robert Kobus is a 30 year non-agent employee of the FBI who disclosed time and attendance fraud by FBI agents. The OIG also conducted an investigation into these allegations and substantiated that he was retaliated against for protected whistleblowing. This retaliation included demoted Mr. Kobus to a non-supervisory position, and even went so far as to move him from his office to a cubicle on the vacant 24th floor of the FBI's office building in New York. Nevertheless, the OIG's findings were then referred to OARM and Mr. Kobus' case has now languished in bureaucratic red tape for approximately 4 years.

These responses are current as of 2/24/12

a. Why has the FBI continued to litigate Mr. Kobus' case despite a finding by the OIG that he was retaliated against?

Response:

The Office of the Inspector General (OIG) made only one specific recommendation for corrective action related to Kobus: that the FBI restore Kobus "to the position of a senior administrative support manager in the New York Field Division, or an equivalent position." That action was taken effective December 23, 2007. The FBI has, though, raised several legal and factual concerns regarding the merits of this case in its briefs to DOJ's OARM. The FBI is awaiting OARM's decision on these issues.

b. Do you agree with the OIG that moving Mr. Kobus to a vacant floor at the New York FBI office constituted retaliation for protected whistleblowing? If not, why not?

Response:

The FBI cannot address the merits of this case at this time because it is currently in litigation, awaiting OARM's decision on several legal and factual issues.

c. Do you believe it is acceptable for any FBI supervisor to move an FBI employee to a vacant floor for any reason, notwithstanding retaliation for protected whistleblowing? If so, please describe when it would be appropriate.

Response:

There are occasions in which operational needs and workspace limitations might necessitate temporarily placing FBI personnel in less than optimal work spaces. We cannot, though, address the issues raised in this case because it is currently in litigation, awaiting OARM's decision on several legal and factual issues.

d. Have you taken any administrative action against Mr. Kobus' supervisors for retaliating against him for protected whistleblowing? If not, why not?

Response:

The FBI takes appropriate administrative and disciplinary action against those found to have engaged in reprisals. As noted above, we are currently awaiting OARM's decision on several legal and factual issues in this case. Determinations regarding appropriate administrative and disciplinary action will be made after those issues are decided.

These responses are current as of 2/24/12

e. Do you agree that 9 years in the Turner case and more than 4 years in the Kobus case are too long and too far removed to be an effective mechanism to get to the bottom of employee retaliation cases? If not, why not?

Response:

As required by law (5 U.S.C. § 2303), the FBI follows procedures published at 28 C.F.R. Part 27 to process, evaluate, and respond to allegations of retaliation against FBI employees. This process can be lengthy, and the FBI continues to assess how we can improve our internal procedures in order to streamline the phases of the process within our control. The FBI cannot, though, take the actions assigned by law to others, including the decision to order corrective action, which is the responsibility of the OARM.

Congressional Access to Line Agents and Attorney's

16. The FBI and Department of Justice routinely sometimes denies Congress access to line FBI agents and prosecutors. Most recently, the Department denied me and Congressman Issa access to line agents and prosecutors as part of our investigation into the ATF's failed Operation Fast & Furious.

Despite arguments from FBI and the Department that this is a "longstanding" policy, it has not been consistently enforced. However, I'm very concerned that a new standard is developing, especially given that the FBI and Department of Justice recently let career prosecutors and FBI agents be interviewed at length on a national television show investigating the Anthrax attacks. Specifically, Assistant U.S. Attorney Rachel Lieber, and FBI agents Jennifer Smith and Edward Montooth were interviewed by PBS' Frontline.

a. Why do the Justice Department and the FBI deny members of Congress access to line agents and attorneys but let them be interviewed at length on television news programs?

b. Will you commit to allowing Congress the same access to FBI agents as you allow the press? If not, why not?

c. How can you justify providing line agents to the media and not to Congress?

Response to subparts a through c:

The Committee is correct that the FBI's Congressional witnesses are typically senior FBI executives and we note that even they are typically not made available for interviews or hearings regarding pending criminal investigations or cases. In addition, our policy with

These responses are current as of 2/24/12

respect to line agents (like line attorneys) is designed to ensure the integrity of our law enforcement efforts and the public perception that they are not susceptible to inappropriate influence. We recognize that line agents may have detailed knowledge of the facts of a given event or investigation, but also note that Congressional questions are not limited to such narrow issues. Senior executives not only have broader experience that enables them to address a wider range of subjects, but they may also be better able to distinguish between matters that are appropriate for FBI comment and matters that should be addressed, instead, by other entities. For many of these same reasons, the FBI generally prefers that senior executives address the media.

In addition to circumstances in which FBI representatives address the Congress or the media in their official capacities, individuals may communicate with either the Congress or the media in their personal capacities. Both of the FBI agents who participated in the news program pertaining to the closed Anthrax investigation were retired from the FBI (Special Agent Jenifer Smith retired from the FBI in January 2009 and Special Agent Ed Montooth retired in May 2011).

Transfer of Ali Mussa Daqduq to Iraq

17. Ali Mussa Daqduq is a Lebanese national and senior Hezbollah commander captured in 2007 and detained in U.S. military custody. Daqduq has been linked to the Iranian government and a brazen raid in which four American soldiers were abducted and killed in the Iraqi holy city of Karbala in 2007.

Recent press reports have indicated that if Daqduq was transferred or moved to the United States to stand trial for his crimes against American citizens, the President believed the proper venue for that trial was a military court.

a. Do you agree with this position, that Daqduq should have been tried in a military tribunal and not an Article III court? If not, why not?

b. Do you support the Administration's decision to transfer Daqduq to Iraq? Was this the correct outcome?

c. Do you believe that Daqduq will face a real criminal trial and, presuming he is found guilty of his crimes, sentencing for his involvement in the deaths of U.S. military servicemen or do you believe that he will ultimately be released by the Iraqis?

Response to subparts a through c:

These responses are current as of 2/24/12

While the FBI investigates criminal activity, we do not prosecute violations and we are not in a position to identify the best forum for prosecution or to assess the likelihood of criminal trial and sentencing in Iraq.

FBI Informant Mark Rossetti

18. On October 17, 2011, I sent a letter to you regarding FBI informant Mark Rossetti. Mr. Rossetti is an alleged "captain" in the New England mafia who, according to media reports, had a close relationship with the Boston FBI. I asked you several questions regarding the FBI's relationship with Mr. Rossetti. You did not respond to my letter, but Mr. Kelly, the Assistant Director of the FBI for Legislative Affairs did respond. In a letter to me he said, "the FBI did not protect any individuals from prosecution in this manner." Then in a subsequent briefing with my staff, FBI agents said that they could not verify the accuracy of that statement.

a. Is the statement in the October 17, 2011, letter from Mr. Kelly correct?

Response:

By letter dated October 17, 2011, Senator Grassley inquired about news reports regarding Mark Rossetti and his status as an FBI informant. Among these news reports is a Boston Globe article dated August 12, 2011, which indicates that Rossetti expected to be spared from prosecution for the crimes he committed with the FBI's knowledge. By letter dated November 17, 2011, Mr. Stephen Kelly, Assistant Director of the FBI's Office of Congressional Affairs, responded to Senator Grassley, quoting the joint statement of the FBI and the Massachusetts State Police in response to the Boston Globe article. Mr. Kelly's response attempted to make clear that, contrary to the suggestions in news reports such as the Boston Globe's, the FBI did not protect Rossetti from prosecution by the Massachusetts State Police but, instead, cooperated with the Massachusetts State Police in their organized crime investigation.

b. The FBI has sent an examination team to look at the Bureau's actions regarding Mr. Rossetti, can you give me an idea of where they are in their investigation and when they will be finished?

Response:

The FBI's Inspection Division is currently conducting a thorough review of the FBI's relationship with Mr. Rossetti. This review includes interviews of those with relevant information (including FBI employees, employees of other federal agencies, and others) and detailed consideration of the case documents and other reporting concerning Mr. Rossetti. The document review was recently concluded and the FBI's Inspection

These responses are current as of 2/24/12

Division is conducting final interviews and drafting its report. Once complete, the report will be reviewed for any information gaps and returned for additional research and revision as necessary. Following approval, the report will be provided to all FBI divisions with an interest in the matter for their information and appropriate corrective action.

Combating Violent Extremism Proposal

19. In a briefing to the Senate Judiciary Committee about the Administration's Combating Violent Extremism (CVE) initiative on December 21, 2011, the FBI representative reported that the FBI established a "CVE Office" at the FBI.

a. What are the duties and goals of this office?

Response:

The FBI has been working to counter violent extremism for many years through a variety of means. We established the Countering Violent Extremism (CVE) Office to improve our effectiveness in empowering our state, local, and community partners to assist in this effort. The duties and goals of this office include the following.

- Developing a better understanding of, and countering the threat of, violent extremism in the United States.
- Strengthening community partnerships and providing to state and local officials and to community leaders unclassified briefings regarding the threat of extremism.
- Addressing CVE-related operational and mission-support needs, including investigations, analysis, and training.
- Coordinating FBI interests with regard to CVE matters with those of other agencies to ensure U.S. Government efforts are aligned.

b. Where does this office fit in the structure and hierarchy at the FBI?

Response:

The CVE Office resides in the FBI's National Security Branch and reports directly to the Executive Assistant Director of that Branch.

c. How many employees are assigned to this office?

These responses are current as of 2/24/12

Response:

Currently four people are assigned to the CVE Office: one Special Agent and Principal Coordinator, two Intelligence Analysts, and one Management and Program Analyst. This staff will be augmented with additional personnel on rotational 60 to 90-day temporary duty assignments. In the coming months, the CVE Office will reevaluate its staffing needs and establish its permanent staffing levels.

d. Do they have duties beyond those in the CVE?**Response:**

No. The duties of those assigned to the CVE Office focus solely on countering violent extremism and threats.

e. How does the FBI define “violent extremism”? Please provide examples of what the FBI views as “violent extremism”.**f. How does the FBI differentiate between “violent extremism” and extremely violent criminal acts?****Response to subparts e and f:**

While a given violent criminal act could be both an “extremely violent act” and an incident of “violent extremism,” the FBI defines violent extremism as committing, or encouraging, condoning, justifying, or supporting the commission of, a violent criminal act to achieve political, ideological, religious, social, or economic goals. In the absence of these or similar activities, thoughts and perspectives that might be viewed as “extreme” are not against the law, even though they may be highly objectionable. Examples of violent extremists include the following.

- James Von Brunn, a self-proclaimed white supremacist, was indicted for murder and related hate crimes and gun charges related to his shooting of a security guard in the United States Holocaust Memorial Museum in Washington, D.C., on June 10, 2009. Von Brunn died of natural causes on January 6, 2010.
- Farooque Ahmed, who received a prison sentence of 23 years after pleading guilty to charges stemming from his attempts to assist others whom he believed to be members of al-Qa’ida in planning multiple bombings designed to cause mass casualties at Metrorail stations in the Washington, D.C., area. Ahmed had suggested where explosives should be placed on trains in Metrorail stations to kill the greatest possible number of people.

These responses are current as of 2/24/12

- Antonio Benjamin Martinez (also known as Muhammad Hussain), who pled guilty to attempting to detonate what he believed to be explosives in a parked vehicle at an Armed Forces recruiting station in Maryland. According to the plea agreement, Martinez spoke about his anger toward America, his belief that Muslims were being unjustly targeted and killed by the American military, and his desire to engage in violence to send a message that American soldiers would be killed unless the country stopped its “war” against Islam.

g. How does this definition influence the FBI’s actions to contribute to the CVE initiative?

Response:

The FBI’s definition of violent extremism guides our development of CVE policy, including our emphasis on improving information sharing, empowering and strengthening community partnerships, and participating in the national CVE strategy. For example, we refer to this definition:

- In our efforts to identify circumstances in which we might engage community organizations and provide them the tools to address CVE issues.
- To identify opportunities to work with our state and local law enforcement partners to identify indicators revealing violent extremist behavior.
- In our work with our foreign partners, to develop cross-comparison analyses with respect to similar characteristics of violent extremism in their countries.

Fort Hood Shooting by Major Hasan

20. During a joint session by the House and Senate Homeland Security Committees on December 7, 2011, Senator Collins discussed a letter she had received from the Department of Defense regarding the shooting by Major Nidal Hassan at Fort Hood. It has been publicly reported that Hassan was in contact with Anwar al-Awlaki—an Islamic extremist member of al Qaeda in the Arab Peninsula—prior to undertaking the horrific attack that killed 13 Americans. In the letter the Department of Defense referred to documents attached to the letter as illustrative of how “the Department is dealing with the threat of violent Islamist extremism in the context of a broader threat of workplace violence.”

a. Do you consider the Fort Hood shooting as an act of terrorism? If not, why not?

Response:

These responses are current as of 2/24/12

In the context of the FBI's investigative authority, terrorism "includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, to further political or social objectives (28 C.F.R. § 0.85(I))." (FBI Domestic Investigations and Operations Guide at § 2.4.2.) While we cannot comment on this case while it is pending, we note that the decision to charge one offense rather than another (such as the decision to charge murder rather than terrorism) depends on a variety of factors. Nidal Hasan has been charged with 13 counts of premeditated murder and 32 counts of attempted premeditated murder.

b. Do you consider Major Nidal Hassan a violent extremist? If not, why not?

Response:

As indicated in response to Question 19e, above, the FBI defines violent extremism as committing, or encouraging, condoning, justifying, or supporting the commission of, a violent criminal act to achieve political, ideological, religious, social, or economic goals. Although we cannot comment on this case while it is pending, we note that the decision to charge one offense rather than another depends of a variety of factors. Nidal Hasan has been charged with 13 counts of premeditated murder and 32 counts of attempted premeditated murder.

c. Do you agree with the characterization of the Fort Hood shooting as "workplace violence"? Why or why not?

Response:

We do not have an opinion as to how DoD characterizes this criminal activity.

Classification of Documents as Sensitive Security Information

21. On November 23, 2011, the FBI sent a memorandum to Congressional Members and Staff of six separate Congressional committees, including the Senate Committee on the Judiciary. This memorandum was stamped "Sensitive Security Information" and included the following warning:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 40 [sic] CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration

These responses are current as of 2/24/12

of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For the U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

a. Why is the FBI utilizing classification authority under 49 CFR parts 15 and 1520, which govern Sensitive Security Information for the Department of Transportation, Federal Highway Administration and the Transportation Security Administration?

b. Does the FBI really authorize the Administrator of the Transportation Security Administration to declassify FBI documents the FBI stamps as Sensitive Security Information under 49 CFR parts 15 and 1520?

c. How many other times has the FBI stamped a document provided to Congressional Committees as Sensitive Security Information under the authority of the Department of Transportation?

Response to subparts a through c:

Memos dated November 23, 2011, were sent to the FBI's Congressional oversight committees as transmittal memos forwarding the recently revised Domestic Investigations and Operations Guide (DIOG). We appreciate the alert to the language quoted above, which was inserted erroneously. The Committee is correct that the Department of Transportation is not involved in establishing handling caveats for FBI materials.

Although erroneous in some administrative respects, the above language correctly identified the DIOG as sensitive. On the DIOG, itself, the Committee would have found the handling caveat that is most clearly and overtly applicable to the DIOG. That handling caveat reads as follows.

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

Questions Posed by Senator Kyl

These responses are current as of 2/24/12

22. After passage of the Cruise Vessel Security and Safety Act of 2010, and pursuant to 46 U.S.C. § 3507(g)(4)(A), cruise ship operators are required to report any criminal activity described in 46 U.S.C. § 3507(g)(3)(A)(i) directly to the FBI. It appears that the FBI, in turn, decides whether to investigate any alleged crimes further. Ultimately, the FBI reports all incidents described in 46 U.S.C. § 3507(g)(3)(A)(i) to the Secretary so that a statistical compilation can be provided to the public on an internet site maintained by the Coast Guard. The statute reads in pertinent part as follows:

The Secretary shall maintain a statistical compilation of all incidents described in paragraph (3)(A)(i) on an Internet site that provides a numerical accounting of the missing persons and alleged crimes recorded in each report filed under paragraph (3)(A)(i) that are no longer under investigation by the Federal Bureau of Investigation.

46 U.S.C. § 3507(g)(4)(A).

Consequently, all alleged crimes that are *not under investigation* are reported — the “no longer under investigation” requirement acting as a necessary condition for an incident to be reported. However, the Coast Guard internet site states that “matters no longer under investigation” do not include “matters that were reported that did not result in open investigations.” *Cruise Vessel Sec. and Safety Act (CVSSA) Statistical Compilation*, U.S. Coast Guard, <http://www.uscg.mil/hq/cg2/cgis/Docs/CruiseLineIncidentsReportingStatsQ32011.pdf>.

One interpretation of this statement would suggest that in its statistical data, the FBI reports only those incidents for which a file was opened. If a file is not opened, the incident does not satisfy the “no longer under investigation” requirement. If this is the case, it is in contradiction to federal law, which requires the FBI to report “all incidents” — not just those for which the FBI opened a file — to the Secretary. 46 U.S.C. § 3507(g)(4)(A).

a. What is the FBI’s process for reporting alleged criminal activity described in 46 U.S.C. § 3507(g)(3)(A)(i) to the Secretary?

Response:

The Cruise Vessel Security and Safety Act (CVSSA) (Pub. L. No. 111-207 (July 27, 2010)) requires the owner of a covered vessel to notify the FBI of occurrences on board the vessel involving “homicide, suspicious death, a missing United States national, kidnapping, assault with serious bodily injury, any offense to which section 2241, 2242, 2243, or 2244(a) or (c) of title 18 applies, firing or tampering with the vessel, or theft of

These responses are current as of 2/24/12

money or property in excess of \$10,000.” (46 U.S.C. § 3507(g)(3)(A)(i).) The owner of the vessel is also required to report these incidents to an Internet-based portal maintained by the Secretary (46 U.S.C. § 3507(g)(3)(A)(ii)). The Secretary is required to maintain on the Internet site “a statistical compilation of all incidents described in paragraph (3)(A)(i) . . . that are no longer under investigation” by the FBI (46 U.S.C. § 3507(g)(4)(A)).

The FBI has no statutory obligation to report to the Secretary, and we do not report “all incidents described in 46 U.S.C. § 3507(g)(3)(A)(i) to the Secretary,” as is indicated in the question. The FBI does, though, provide to the Secretary a quarterly statistical report reflecting the number of cases closed during the quarter that stemmed from one of the above serious violations. This number does not match the other numbers reported for that quarter for a couple of reasons. First, cases are typically not closed in the same quarter in which they were reported to the FBI. Second, the FBI does not open cases on all of the alleged incidents reported to us under 46 U.S.C. § 3507(g)(3)(A)(i). Often these are sexual offenses in which late reporting has caused a loss of physical evidence or a contaminated crime scene. In other cases, the next port of call or other country exercising primary jurisdiction has delayed investigation or intervened in a way that affects the FBI’s ability to conduct a thorough investigation.

b. Does the FBI report all alleged incidents of such criminal activity to the Secretary, or does the FBI report only those incidents for which a file was opened? If the latter, why?

Response:

Each quarter, the FBI reports the number of cases closed during the quarter that stemmed from one of the serious violations listed in 46 U.S.C. § 3507(g)(3)(A)(i). The CVSSA requires that the owners of covered vessels report specified information to the FBI, that these owners report specified information to an Internet portal maintained by the Secretary, and that the Secretary maintain a statistical compilation on the Internet. These are the only statutory reporting requirements.

23. FBI data for 2010 shows that 35 instances of relevant criminal activity took place on-board cruise ships in 2010. Through the first three quarters of 2011, FBI data indicates only 13 occurrences of relevant criminal activity, including *not a single instance* for the most recent quarter, July 2011 to September 2011. In isolation, this drop in criminal activity seems improbable, but it seems even less likely when considering data obtained from the FBI by the *Sun Sentinel*. http://databases.sun-sentinel.com/news/broward/ftlaudcruise/ftlaudcruise_list.php.

These responses are current as of 2/24/12

From December 2007 to October 2008 — a period covering only 11 months — the *Sun Sentinel* reports 363 instances of criminal activity on-board cruise ships. While it is true that some of these crimes would not be reported under the 2010 Cruise Vessel Security and Safety Act, it nevertheless illustrates the large discrepancy in the number of relevant crimes reported by the FBI between 2008, 2010, and 2011. In particular, the fact that zero relevant crimes took place in the third quarter of 2011 appears to be far outside the statistical norm. It seems improbable that there were no reportable instances of criminal activity for the latest quarter for which data is available.

What explanation can the FBI give for the large discrepancies in the number of crimes reported for 2008, 2010, and 2011?

Response:

The number reported by the FBI for a given quarter represents the number of cases closed (“no longer under investigation” by the FBI, pursuant to 46 U.S.C. § 3507(g)(4)(A)) among the serious cases reported pursuant to 46 U.S.C. § 3507(g)(3)(A)(i). This number does not represent the total number of offenses occurring on cruise ships during the quarter, or even the number of serious offenses during that period.

24. Does the FBI have any reason why not a single instance of pertinent criminal activity was reported for the third quarter of 2011?

Response:

As indicated above, the number reported by the FBI for a given quarter represents the number of serious cases closed during that quarter. This number does not represent the total number of offenses occurring on cruise ships during the quarter, or even the number of serious offenses during that period. If the FBI reports no activity during a given quarter, this means that none of the serious cases reported to the FBI under 46 U.S.C. § 3507(g)(3)(A)(i) were closed during that quarter. The FBI closed none of these serious cases during the 3rd quarter of 2011.

Questions Posed by Senator Sessions

25. You have testified on numerous occasions that the shift of 2000 agents to national security following September 11th left the Bureau with a reduced ability to investigate criminal cases. According to statistics provided by the FBI to my staff, in FY06 there were a total of 12,663 special agents; for FY11, there were a total of 13,910 special agents – an increase of 1,247 in the total onboard Special Agent population. Have any of these new

These responses are current as of 2/24/12

hires been assigned to backfill the positions in the white collar crime program? Please provide a breakdown of the programs to which the new agents have been assigned.

Response:

It is often difficult to compare numbers obtained in response to requests seeking different information. The increase in Special Agent (SA) positions of 1,247 that is referenced in the question includes both "direct hires" (those SAs who are new FBI employees) and reimbursable SA positions (individuals from other agencies who are not FBI employees but who are temporarily doing FBI work and whose salaries are paid by the FBI). Of these 1,247, 656 are direct hire SAs and include 131 white collar crime positions expressly provided for by Congress from FY 2006 to FY 2011 (25 SA positions specifically for financial crime investigations provided for in FY 2009, 25 positions in FY 2010, and 81 positions in the FY 2009 Financial Crimes Supplemental Appropriation). FBI records that capture the types of investigations worked by all FBI agents (both direct hires and those on reimbursable details, as described above) indicate that, during the period of FY 2006 to FY 2011, the number of agents investigating white collar crime matters has increased from 1,505 in FY 2006 to 1,659 in FY 2011, an increase of 154 positions or approximately 10 percent.

26. On December 8, 2011, the Senate Environment and Public Works Committee passed a resolution, which I opposed, to direct the General Services Administration (GSA) to pursue a lease for a new FBI Headquarters building somewhere in the greater Washington, D.C. area. This was prompted by a Government Accountability Office (GAO) report that concluded that the FBI needs a new headquarters building with over two million square feet of office space on at least 55 acres to accommodate 11,500 employees at a cost of \$1.5 billion.

a. Why does the FBI headquarters need to be in the greater Washington, D.C. area?

Response:

Space in the Washington, D.C., area is expensive, and we are seeking ways to minimize the cost of FBI office space. For example, currently several elements of FBIHQ are located outside the metropolitan area. This is possible because these elements engage in less frequent direct coordination with other FBIHQ elements and others in the D.C. law enforcement and intelligence communities. These elements include the FBI's Criminal Justice Information Services Division, Laboratory Division, Training Division, Operational Technology Division, Records Management Division, and Hazardous Devices School.

These responses are current as of 2/24/12

b. Why do all FBI headquarters personnel need to be centrally located in one building?

Response:

A consolidated FBIHQ facility would enhance efficiency. This is, therefore, among the alternatives being considered. Only 52 percent of FBIHQ employees are currently housed in the J. Edgar Hoover (JEH) building because of space limitations, requiring the FBI to acquire space in approximately 20 other locations. While the FBI would ideally realign organizational elements and adjust their staffing to quickly address shifts in our mission and changes in the threats we are addressing, this is both time consuming and costly when the organizational elements involved are housed in different locations.

c. Based on the figures in the GAO report, headquarters personnel has increased 78% since 2001 when you became Director. What accounts for that increase?

Response:

The FBI has changed a great deal since the attacks of 9/11. In concert with the significant changes in the United States Intelligence Community, the FBI has increased its intelligence capabilities and has established the infrastructure needed to support this increase. Among other things, since 2001 the FBI has created a National Security Branch, Directorate of Intelligence, Cyber Division, Weapons of Mass Destruction Division, and Special Technologies and Applications Office. In support of these capacities, we have worked to ensure that our infrastructure can continue to support FBI functions. This has required the an increase in Information Technology personnel and a Resource Planning Office, as well as significant growth in our Security Division, Human Resources Division, Facilities and Logistics Services Division, and Office of the General Counsel.

27. You testified that the detainee provisions in the National Defense Authorization Act for Fiscal Year 2012 (NDAA) create a problem for the FBI in the following hypothetical: the FBI arrests three people, one of whom is a United States citizen and two of whom are subject to mandatory military detention.

a. Do you agree that, under the provisions in the NDAA, military custody of the United States citizen is permitted but not mandatory, such that all three hypothetical arrestees could be detained in military custody, if necessary?

Response:

These responses are current as of 2/24/12

Pursuant to section 1022(b) of the National Defense Authorization Act (NDAA) (Pub. L. 112-81), the “requirement to detain a person in military custody under this section does not extend to citizens of the United States.” Whether the 2001 Authorization for Use of Military Force (AUMF) would authorize the military custody of a United States citizen arrested by the FBI inside the United States would depend on the specific factual circumstances and would raise legal issues that have not been resolved by the courts or clarified by the NDAA. Indeed, section 1021(e) of the NDAA provides that section 1021’s affirmation of detention authority granted by the AUMF does not “affect existing law or authorities relating to the detention of United States citizens, lawful resident aliens of the United States, or any other persons who are captured or arrested in the United States.”

b. Do you acknowledge that, under these provisions, the president could provide a waiver to keep the two arrestees subject to mandatory military detention in civilian custody if it is in the interests of national security?

Response:

Yes. Section 1022(a)(4) of the NDAA provides that the President may waive the military custody requirement if such a waiver is in the interests of national security and Section 1022(d) specifically states that “[n]othing in this section shall be construed to affect the existing criminal enforcement and national security authorities of the Federal Bureau of Investigation or any other domestic law enforcement agency with regard to a covered person, regardless [of] whether such covered person is held in military custody.” Pursuant to Presidential Policy Directive (PPD) 14, subject: “Procedures implementing Section 1022 of the National Defense Authorization Act for Fiscal Year (FY) 2012” (February 28, 2012), the military custody requirements of NDAA Section 1022(a)(1) are categorically waived, for example, when “transferring an individual to U.S. military custody could interfere with efforts to secure an individual’s cooperation or confession” (PPD 14 at para. II.B.6) or when “transferring an individual to U.S. military custody could interfere with efforts to conduct joint trials with co-defendants who are ineligible for U.S. military custody or as to whom a determination has already been made to proceed with a prosecution in a Federal or State court” (PPD 14 at para. II.B.7). In addition, the Attorney General may, in consultation with other senior national security officials, waive the requirements of NDAA Section 1022(a)(1) in the national security interests of the United States on a case-by-case basis (PPD 14 at para. II.D).

28. Recent reports published by the Department of Treasury indicate that officials at the Office of Thrift Supervision (OTS) either directed or acquiesced in the backdating of capital contributions by the thrifts they were responsible for regulating. Regional Director Darrell Dochow approved the backdating of \$18 million by IndyMac, and Senior Deputy Director Scott Polakoff and two other OTS officials directed BankUnited to backdate \$80

These responses are current as of 2/24/12

million in capital contributions. Although an investigation of IndyMac was initiated in 2008, no charges have been filed against former Dochow, Polakoff, or the other officials involved in the BankUnited case.

a. I understand that in 2008 the FBI was investigating IndyMac. Can you comment on the scope or nature of that investigation and whether it included the OTS officials' involvement in the backdating of documents?

b. Is the FBI investigating the officials who directed the backdating of documents in the BankUnited matter? If so, can you comment on the scope or nature of that investigation?

Response to subparts a and b:

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, witness tampering, or other activity that would impede an FBI investigation.

Questions Posed by Senator Coburn

29. In October 2010, the Department of Justice Inspector General reported that the FBI's electronic case management system ("Sentinel") cost taxpayers at least \$450 million, and was running two years behind and costing an additional \$100 million.

a. What is the FBI doing to make sure federal funds designated for technology are being spent wisely and effectively?

Response:

Although the October 2010 report by DOJ's OIG indicates that Sentinel is \$100 million over budget, we anticipate that, when delivered with full functionality, the program will be within the \$451 million budget and will include the capability originally envisioned.

The FBI works to ensure its technology funds are apportioned to meet its resource needs with maximum efficiency. As the first step in this effort, the FBI's Information Technology (IT) Strategic Plan defines high-level long-term business goals and objectives that support the Strategic Plan and Strategy Management System goals. Assisted by FBI project managers, functional experts (such as systems engineers), cost performance specialists, and financial analysts, executive-level managers assess a

These responses are current as of 2/24/12

proposed project's anticipated size, complexity, risk, criticality, type of contract, and other factors to select the performance management methodology and reporting best suited to effective management of that particular project.

In order to enhance efficiency, the FBI is currently revising its approach to system life cycle management (LCM), using industry best practices to forge new IT Governance and LCM practices and to strengthen and enhance agile development approaches within the FBI. The IT Governance framework drives the executive-level oversight necessary to maintain alignment between the FBI's investments, projects, and mission priorities. This framework ensures that IT investments are prioritized properly and that IT projects comport with the FBI's LCM framework so that senior executives provide clear guidance and decisions are made in a timely manner and at the right level.

b. What is the FBI doing to ensure that its future technology contracts stay on course and do not exceed projected costs?

Response:

Several aspects of the FBI's IT program combine to ensure timely and cost-effective completion of the FBI's IT projects.

First, the FBI employs an Earned Value Management (EVM) methodology in support of integrated program management for capital investment programs and projects. This methodology provides the FBI and its vendors with timely, accurate, and integrated cost, schedule, and technical performance information. Under the EVM methodology, achievement is objectively measured against established goals in a performance baseline plan on a periodic basis, helping to ensure that programs and projects stay on course. This periodic evaluation helps to identify potential cost and schedule problems early, before they become unmanageable or unrecoverable. This methodology has proven to be a highly effective management tool.

In addition to EVM, the use of the Independent Verification and Validation Program for high-dollar critical projects has helped to increase performance, promote compliance with established policies, procedures, and regulations, and increase visibility into FBI processes. This program adds additional objectivity to the evaluation process and recommends mitigation when risks are discovered.

The FBI has worked hard to develop a strong cadre of IT program managers (PMs) who hold the Federal Acquisition Certification for Program and Project Managers. These well-trained and experienced PMs work to ensure that the FBI's projects are delivered on time and within budget.

These responses are current as of 2/24/12

30. Since 9/11, the FBI has worked to transform itself into a pro-active intelligence-focused organization. Thus, it must now balance its resources between intelligence deployed to the field (to work with and support investigations) and headquarters to conduct “strategic analysis.”

a. What share of FBI intelligence spending is occurring at headquarters?

Response:

Because of the FBI’s transformation since the attacks of 9/11, garnering intelligence is now a key component in every investigation. This is true regardless of whether the investigation concerns terrorism, gang crimes, cyber crimes, or other matters under FBI jurisdiction. It is the mission of the FBI’s Directorate of Intelligence (DI) to collect, produce, and disseminate actionable intelligence that enables the FBI to identify and counter current and emerging threats. The DI satisfies this mission through intelligence elements embedded both in FBIHQ Divisions and in each FBI field office. Although in FY 2012 approximately 44 percent of the DI’s resources are located at FBIHQ, these elements are designed to provide critical support and direction to the field.

b. What is the value of the FBI’s strategic intelligence program?

Response:

Strategic intelligence is used by the FBI to allocate resources and techniques in order to exert the greatest possible influence or disruptive impact on priority threats facing the United States and to assist in identifying emerging threats. Strategic analysts cull through and synthesize intelligence collected by a variety of domestic and foreign law enforcement and intelligence services to enhance our understanding of threats, gaps, and vulnerabilities that impact U.S. national security interests worldwide. Analysis of this intelligence is contained in finished intelligence products that are disseminated throughout the FBI and to our Federal, State, local, tribal, and Intelligence Community partners.

Like their strategic analytic colleagues, tactical analysts also work to identify threats and identify intelligence collection needs. Tactical analysts in our field offices are embedded on investigative squads where they work in concert with Special Agents to identify threats and opportunities for intelligence collection in their regional areas of responsibility. Finished intelligence products prepared by tactical analysts are generally not distributed outside the FBI since they are often specific to substantive investigations. Tactical analysts are, though, responsible for raw intelligence reports and situational intelligence reports, which are shared with Federal, State, local, tribal, Intelligence Community, and foreign partners, as appropriate.

These responses are current as of 2/24/12

c. Should more or fewer intelligence assets be deployed to the field to support investigations?

Response:

The FBI's transformation into a threat-based, intelligence-driven organization has led to a dramatic increase in domain analysis, collection management, source identification, and the dissemination of both raw intelligence and finished intelligence products. All of these functions require analytic resources. The FBI is working to determine how our analytic assets can be most efficiently deployed and is exploring all avenues to address this need, including the identification of any areas in which FBIHQ resources can support field operations remotely.

d. What is the FBI doing to measure or quantify the value provided by strategic analysts compared to the analyst working in the field?

Response:

The physical location of an analyst does not determine whether analysis is strategic or tactical. Regardless of whether an FBI intelligence analyst is located in the DI, an operational division, or a field office, the analyst is performing strategic analysis if the intelligence analysis contributes directly to the development of FBI strategy for exerting the greatest possible influence or disruptive impact on our priority threats.

The FBI's DI emphasizes consumer feedback on all strategic analytic products. Customer satisfaction surveys are attached to intelligence assessments, bulletins, and studies, asking that completed surveys be returned to intelligence managers. A similar survey is used to seek evaluation of our Unclassified intelligence products by our state, local, tribal, and private sector partners. Feedback is also conveyed orally and is often accompanied by requests for additional information, briefings, or written analytic products.

The FBI Director receives frequent strategic intelligence briefings, which are also attended by both intelligence and operational executives. These briefings provide an opportunity for immediate strategic and policy input from the FBI's most senior leaders. FBI intelligence analysts are also involved in daily intelligence briefings of the Director and operational division executive managers, and many field office intelligence analysts brief their Special Agents in Charge frequently, as well. Since intelligence analysis supports FBI operations and policy at both the strategic and tactical levels, this frequent interaction provides a steady flow of feedback and qualitative assessment of the intelligence value.

These responses are current as of 2/24/12

31. In November 8, 2011, the Government Accountability Office issued a report which found that, according to FBI and GSA assessments, the FBI's headquarters facilities—the Hoover Building and the headquarters annexes—do not fully support the FBI's long-term security, space, and building condition requirements. The GAO report notes that the options for the FBI and GSA are to (1) Modernize the Hoover Building and consolidate outside leases, (2) Demolish the Hoover Building and build a new building at the existing site, or (3) Build a new consolidated headquarters facility on a new site. Option 1 is estimated to take fourteen years, option 2 nine years, and option 3 seven years. Cost estimates for each of the options vary from \$1.7 billion for option 1, \$850 million for option 2, and \$1.2 billion for option 3, but those numbers were largely calculated in 2006-2007 and could be much more today.

a. Given those three choices, which one would be your preferred option?

Response:

Please see the response to Question 26b, above.

b. Do you know why maintenance has been deferred?

Response:

Although the General Services Administration (GSA) is responsible for capital improvements, which include systems replacement, GSA has delegated building operations and maintenance to the FBI. Little of that maintenance is deferred.

c. Where could budget cuts be made to allow for such a large federal expenditure to build a new FBI headquarters?

Response:

The FBI is not the expert on the best vehicles for funding projects of this type. We will be pleased to work with the Congress, GSA, and other stakeholders to address our facility needs in the most cost effective way possible.

32. a. What is the FBI doing to ensure that its overall resources are being spent effectively?

Response:

These responses are current as of 2/24/12

The FBI takes several measures to ensure its resources are expended efficiently and effectively, continually looking for cost saving opportunities and improvements in business practices that would make the FBI more efficient. For example, the FBI created a capital planning office to provide a comprehensive and objective analysis of major investments with a strategic long-term focus. In addition, the FBI's Finance Division (FD) conducts semi-annual "spend plan" reviews and meets with each division to ensure that programs are adequately funded and budgets are efficiently executed, and FBI Divisions conduct their own internal reviews to ensure their funds are expended in accordance with FBI priorities. Twice a year, Field Offices participate in Strategy Performance Sessions, which are a means by which program progress, challenges, and opportunities related to performance and threats can be assessed, further assisting executive managers in making efficient resource allocations. Each quarter, the FD provides to the leadership of each division data on the division's effectiveness in managing its funding, contracts, and assets. The FD reviews program spending with each division, recommends efficiencies, and investigates possible duplications of effort. These reviews of our funding and contract activities have led to several program changes. For example, the FBI has: implemented several efficiencies in the procurement process that have yielded significant cost avoidances and savings, including the creation of a "costing and pricing team" that has identified millions of dollars in potential savings on pending contract awards; increased the emphasis on acquisition planning and improved statements of work, resulting in more accurate independent government cost estimates and a better framework for identifying and eliminating unnecessary cost drivers before entering into negotiations and during contract performance; converted critical contractors to FBI employees, thus lowering turnover rates and preventing the loss of intellectual capital needed to execute the FBI's mission and to support DOJ, OMB, and ODNI priorities; and renegotiated existing contracts before option years were exercised.

b. Does the Bureau encourage "use or lose" budget spending?

Response:

The FBI does not encourage "use or lose" budget spending but, instead, leverages the "spend plan" process described above to ensure that appropriated funds are spent appropriately, effectively, and efficiently.

Because the threat landscape is constantly evolving, the FBI must also continuously evaluate the funding levels for priority programs. If critical programs are underfunded, reprogramming notifications will be submitted to Congress so that we can shift resources from lower priority programs to address shortfalls in these critical programs.

c. What is the FBI doing to prepare for future budget cuts?

These responses are current as of 2/24/12

Response:

If there should be a sequestration, the FBI would likely face \$650 million to \$800 million in budget cuts, which is approximately 8.5 to 10 percent of the FBI's annual appropriation. A budget cut of this magnitude could not be absorbed through efficiency savings alone. Sequestration would impact the FBI's mission and could result in reductions in investigative operations and infrastructure, a bureau-wide furlough, and a lengthy hiring freeze.

As a DOJ component, the FBI would participate in the Department-wide 25-workday furlough, resulting in a decrease of approximately 3,500 Special Agent, Intelligence Analyst, and Professional Staff work years. In addition to the negative impact on employee productivity and morale, a hiring freeze and furlough of this length would likely disrupt national security and criminal investigations, intelligence collection and dissemination, and surveillance capabilities.

d. Could any of the divisions at the headquarters be streamlined to be more efficient without jeopardizing the Bureau's ability to perform its core mission in the field? If so, which divisions?

Response:

The FBI has already streamlined many of its processes and procedures and has implemented a strategic and financial management framework that aligns FBI priorities with funding sources. This framework – the Strategy Management System – facilitates objective and strategic resource allocation decisions, providing the tools to monitor strategic performance and creating a vehicle for holding our leaders and managers accountable for specific performance objectives and initiatives.

33. a. What is the turnover rate in the FBI's different divisions?

Response:

The FY 2011 turnover rate for FBIHQ divisions was 5.0 percent, while it was 3.4 percent for field divisions. The turnover rate for FBIHQ divisions was slightly higher than for field divisions because certain FBIHQ support employees were offered voluntary early retirement during FY 2011.

b. What is the turnover among various kinds of employees—agents, analysts, other support personnel?

Response:

These responses are current as of 2/24/12

The FY 2011 turnover rates for the specified employee categories were as follows.

Special Agents	3.1 percent
Intelligence Analysts	4.3 percent
Other support personnel	4.6 percent

The turnover rate for “other support personnel” was elevated slightly by the fact that certain FBIHQ support employees were offered voluntary early retirement during FY 2011.

c. Do high turnover rates cost the government more money due to the cost of frequently training new, replacement employees?

Response:

Training new employees is particularly costly when turnover rates are high. The FBI is fortunate to have a relatively low rate of turnover.

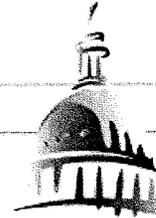
d. What is the FBI doing to ensure it retains the best employees?

Response:

In order to retain employees in hard-to-fill positions and locations, the FBI offers retention incentives under statutory authorities provided by the Congress and regulations promulgated by the U.S. Office of Personnel Management. These authorities require that the employee have unusually high or unique qualifications or that a special need of the FBI for the employee’s service makes it essential to retain the employee. These requirements apply equally to all FBI employees, including Special Agents, Intelligence Analysts, and other Professional Support employees. In addition to retention incentives, the FBI has established a Leadership Development Program designed to support the FBI’s succession planning efforts by preparing employees for leadership roles.

These responses are current as of 2/24/12

SUBMISSIONS FOR THE RECORD

*United States Senator Chuck Grassley**Iowa*<http://grassley.senate.gov>

Prepared Statement of Ranking Member Grassley of Iowa
U.S. Senate Committee on the Judiciary
FBI Oversight Hearing
Wednesday, December 14, 2011

Chairman Leahy, thank you for calling this oversight hearing today. It has been five months since Congress passed and President Obama signed into law an unprecedented two-year extension of Director Mueller's term as Director of the Federal Bureau of Investigation (FBI). Given the historical problems with the FBI amassing too much power, the President's request to extend Director Mueller's term for an additional two-years, breaking from over thirty-five years of practice limiting the Director to a ten-year term, was not a decision I took lightly. Ultimately, given the President's failure to nominate a replacement in a timely and responsible manner, I reluctantly agreed to the request provided we built a historic record that modifying the Directors term was a one-time event.

I'm pleased that Chairman Leahy and members of the Committee agreed with me and moved the extension through regular order including a hearing on the legislation, an executive mark-up of the legislation, floor consideration of the legislation, a new nomination from the President, along with a final confirmation vote. This process sets the historical record that extending Director Mueller's term was not a fly-by-night decision. It also puts the President on notice to begin the process of selecting and nominating a new FBI Director earlier than the last attempt. Another extension will not occur. So, it would be irresponsible not to begin planning sooner rather than later for Director Mueller's inevitable exit.

That said, I want to welcome Director Mueller here today. Director Mueller's tenure as FBI Director has been a good one and his dedication and reputation were significant factors in his 100-0 confirmation vote this past July. I'm sure when his two-year extension runs out he'll be ready for some much needed downtime and will look forward to transitioning the office to his successor.

With regard to policy matters, there are a number of topics I intend to discuss with the Director. First, I want to discuss a perpetual problem at the FBI, whistleblower protection. I have raised this issue with the Director repeatedly during his tenure, but it continues to plague the FBI. Director Mueller has repeatedly assured me that he will not tolerate retaliation of any whistleblowing at the FBI. Despite these assurances, two particular whistleblower cases have been dragging on for years. These cases are largely fueled by the FBI's desire to continually appeal rulings and findings of wrongdoing by FBI supervisors.

For example, FBI Agent Jane Turner filed a whistleblower complaint in 2002 when she discovered that FBI agents were removing items from Ground Zero following 9/11. The agents were collecting items from the 9/11 crime scene as personal memorabilia. She faced retaliation for raising concerns about these agents and her case has been stuck in administrative limbo at the Justice Department for over nine years. This is despite the fact she won a jury trial in Federal District Court where the FBI was ordered to pay nearly half a million dollars in damages, in addition to a Justice Department administrative ruling substantiating her claims of retaliation. Even though she has won twice, the FBI recently appealed the case to the Deputy Attorney General who remanded it for further proceedings. Nine years is far too long for any case to be resolved—especially a whistleblower case.

In another case, that of Robert Kobus, a 30-year non-agent employee of the FBI who disclosed time and attendance fraud, the case has languished for over 5 years. This case is similar in that the Inspector General issued a 70 page investigative report detailing the retaliation that Mr. Kobus faced—including being reassigned to a vacant floor at a New York FBI Field Office. Again, the FBI has continued to appeal this case despite clear findings of retaliation.

I wrote to Attorney General Holder last month about these cases pointing out statements made by the Attorney General and Deputy Attorney General to support whistleblowers. Those statements are similar to assurances given by Director Mueller. But, like nearly all my inquiries on these cases, the Attorney General's response from his Assistant Attorney General for Legislative Affairs simply provided me a recitation of the appeals process for FBI whistleblowers. Actions speak louder than words. And if the Attorney General, Deputy Attorney General, and FBI Director truly wish to help whistleblowers, they have the power to end the years of appeals and accept the findings issued by the Inspector General and Office of Attorney Recruitment and Management. I intend to ask the Director why he continues to allow the FBI to file appeal after appeal despite clear findings of retaliation. He has the power to end this cycle and show whistleblowers that the FBI and Department of Justice take their complaints seriously.

Anthrax Investigation (Amerithrax):

I also want to discuss some issues that have recently arisen as follow-up to the FBI's closing of the Amerithrax investigation. Specifically, the Justice Department recently settled a wrongful death lawsuit in Florida for \$2.5 million. That suit was filed by the family of an editor who died as a result of the 2001 anthrax attacks. The lawsuit raised questions in the press given potentially conflicting statements made by the Justice Department that seemed to cast doubt on Dr. Ivins' ability to actually manufacture the Anthrax. Additionally, in subsequent depositions of Dr. Ivins' coworkers, statements were made calling into question Dr. Ivins' ability to produce the anthrax used in the attacks given his lack of access to necessary equipment. Ultimately, the Department filed a supplemental filing correcting statements that seemed to cast doubt upon the FBI's case, but did not seek to refute the depositions of Dr. Ivins' coworkers.

I wrote to the Attorney General and the FBI Director in August asking how the Department's filing and the depositions could be squared against the FBI's contention that Dr. Ivins was the sole assailant. In the response, the Justice Department argued that the "issue raised by the United

States in its motion did not pertain to whether Dr. Ivins was responsible for the anthrax attacks or whether he could have created the anthrax powder in his laboratory.” The Department instead argued, “The issue raised by our motion is whether the Army failed to properly oversee and supervise operations at the United States Army Medical Institute for Infectious Disease (USAMRIID) such that the agency was negligent in failing to anticipate and prevent the theft of liquid anthrax and its conversion into powder for use in the attacks.” With regard to the depositions, the Department argued, “doubts of [Dr. Ivins’] colleagues only underscore [DOJ’s] view that Dr. Ivins’ actions were not foreseeable under Florida tort law.” While these statements attempt to thread the needle about the Government’s liability, the fact remains that the Government ended up paying \$2.5 million to settle the case and cast a further cloud on the FBI’s case that Dr. Ivins’ was the sole perpetrator.

Access to Line Agents and Attorneys:

The Anthrax investigation and the Department’s response to it have also raised additional questions. Notably, in responding to press accounts questioning the Government’s case against Dr. Ivins, the FBI and Department both allowed line agents and attorneys to be interviewed on national television. In allowing these FBI agents and Assistant U.S. Attorney’s to conduct detailed interviews with the press, the FBI and Department have provided greater access to the press than they have Congress. Both the Department and FBI routinely argue that line agents and attorneys are prohibited from talking to members of Congress. Yet, you can turn on a television and see in-depth interviews with these same agents and attorneys that members of Congress would like to interview. This has been a very important part of my investigation of the Department’s failed handling of the ATF’s Operation Fast & Furious. I want to know from Director Mueller why he allows line agents to provide detailed interviews to the press on national television, but repeatedly refuses to let Congress and their staff interview line agents and attorneys.

Anthrax Investigation Leaks:

The Anthrax investigation also spurned an unfortunate situation where someone in the Justice Department leaked sensitive information regarding the investigation to the press. Those leaks involved alerting the media that Dr. Steven Hatfill was under investigation and that search warrants were going to be executed on his residence. Ultimately, Dr. Hatfill was exonerated of any wrongdoing in the case, and the Department of Justice settled a civil lawsuit filed by Dr. Hatfill based upon the Department’s violation of the Privacy Act. This settlement cost the American taxpayers nearly \$6 million and occurred based upon the Department’s leak of information to the press. I have repeatedly asked for a status update on the investigation into the leak to determine who the source was.

In response to my August 31, 2011, letter, the Department stated, “After an extensive investigation, career prosecutors concluded that, based upon the Principles of Federal Prosecution, criminal charges were not appropriate in this matter.” This is a stunning development and only adds to concerns I have that leakers at the Justice Department are held to a different standard than Federal employees outside the Department. Now that it appears that the investigation is over, I want to know from Director Mueller who the leakers were and whether

they faced any administrative sanctions for the leaks. The actions of these individuals put federal taxpayers on the hook for a \$6 million settlement; they need to be held accountable.

Another area of concern is the FBI's relationship with informants. The Bureau's actions regarding Whitey Bulger were a black eye for the FBI and recent press reports from Boston indicate that a similarly cozy relationship may have developed between alleged mobster Mark Rossetti and the Boston FBI. I wrote Director Mueller a letter on Mr. Rossetti on October 17th and I look forward to asking him more questions on this matter today.

I would also like to note, that today is the one-year anniversary of the tragic shooting of Border Patrol Agent Brian Terry. My investigation into the ATF's failed Operation Fast & Furious continues. I sent Director Mueller a letter dated October 20, 2011, asking some questions about the FBI's investigation of the murder of Agent Terry. I have not yet received a response to that letter, but I have talked with Director Mueller about the case. I want a commitment from Director Mueller that my letter will be answered in writing. The Terry Family deserves answers about Agent Terry's murder and answering my letter is another step toward getting those answers.

Time permitting, I'd also like to ask the Director about his involvement in the drafting of a memorandum that was reported in the press regarding the targeted killing of Anwar al-Awlaqi, the potential transfer of known enemy combatant Ali Mussa Daquduq from U.S. military custody to Iraq, FBI involvement in investigating mortgage fraud at Countrywide Financial, conflicts between the FBI and agents of the Department of Homeland Security Inspector General investigating corruption among DHS officers at the border, and about the recent Government Accountability Office report on the status of the FBI's headquarters in Washington, D.C.

There is a lot to cover so I look forward to Director Mueller's testimony and his responses to these important matters. Thank you.

PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN
 DIANNE FEINSTEIN, CALIFORNIA
 CHARLES E. SCHUMER, NEW YORK
 RICHARD J. DURBIN, ILLINOIS
 SHELDON WHITEHOUSE, RHODE ISLAND
 AMY KLOBUCHAR, MINNESOTA
 AL FRANKEN, MINNESOTA
 CHRISTOPHER A. COONS, DELAWARE
 RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
 ORRIN G. HATCH, UTAH
 JON KYL, ARIZONA
 JEFF SESSIONS, ALABAMA
 LINDSEY O. GRAHAM, SOUTH CAROLINA
 JOHN CORNYN, TEXAS
 MICHAEL S. LEE, UTAH
 TOM COBURN, OKLAHOMA

United States Senate

COMMITTEE ON THE JUDICIARY
 WASHINGTON, DC 20510-6275

August 31, 2011

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

Via Electronic Transmission

The Honorable Eric H. Holder
 Attorney General
 U.S. Department of Justice
 950 Pennsylvania Avenue, N.W.
 Washington, DC 20530

The Honorable Robert S. Mueller, III
 Director
 Federal Bureau of Investigation
 935 Pennsylvania Avenue, N.W.
 Washington, D.C. 20535

Dear Attorney General Holder and Director Mueller:

I write to express my concerns regarding recent legal developments involving the anthrax-laced letters the Federal Bureau of Investigation (FBI) alleges were mailed by Army scientist Bruce Ivins in 2001. It is my understanding that the Department of Justice (DOJ), in attempting to defend the government from a wrongful death suit filed by one of the victims of the 2001 anthrax attacks, filed documents in the Federal District Court for the Southern District of Florida that seemingly contradicted previous information provided to congressional leadership and the American people. These court documents initially indicated that the DOJ no longer believed that Dr. Ivins created refined anthrax powder in his laboratory. This information seemed to directly refute previous investigative information uncovered by the FBI which specifically identified his access to specialized laboratory equipment as a justification for the investigation of Dr. Ivins, and evidence that he was the lone suspect and would be found guilty beyond a reasonable doubt.

However, after the filing was made public and the differing positions were highlighted by the media, the DOJ subsequently filed court documents and attempted to retract the information that appeared to dispute the FBI's investigation of Dr. Ivins. The DOJ clarified that Dr. Ivins did in fact possess a machine, referred to in court documents as a lyophilizer, which could be used to dry anthrax spores. Nevertheless, the lyophilizer was not directly located in his laboratory, and scientific colleagues that worked with Dr. Ivins continue to assert in sworn depositions that it was virtually impossible for Ivins to create anthrax spores in his laboratory. While DOJ was ultimately successful in amending its filing in this civil case, the sworn depositions of two government employees continue to contradict the FBI's case that Dr. Ivins could have produced anthrax.

The FBI has consistently asserted that Dr. Ivins created anthrax powder in his laboratory while he was employed at the U.S. Army Medical Research Institute of Infectious Diseases at Fort Detrick, MD. This allegation was based in part on Dr. Ivins' access to specialized equipment. Moreover, the FBI emphasized that Dr. Ivins laboratory time significantly increased prior to the mailing of the letters, thus enhancing the circumstantial evidence of the investigation.

Unfortunately, the DOJ and FBI never obtained a criminal indictment of Dr. Ivins prior to his suicide in 2008.

My concern is accentuated by the apparent contradiction of the DOJ court documents to the original FBI investigation, the subsequent attempt to retract that information and the federal judge's ruling that the DOJ Civil Division "show good cause" to justify a modification to the original court filing. The DOJ original court filing seemingly eliminated the FBI's previous circumstantial evidence associated with Dr. Ivins without providing any additional insight as to the means and methodology he may have used to create the anthrax powder. This is particularly troubling given the February 2011 report by the National Academy of Sciences which questioned the FBI's previous analysis correlating the mailed anthrax to that of the supply maintained by Dr. Ivins in his laboratory.

While I recognize the FBI has concluded their investigation into the matter, the recent confusion created by the DOJ has produced a new set of questions regarding this unsolved crime. Consequently, I request that the DOJ and the FBI provide a briefing to my staff so that I may better understand the situation and determine why it appears, at the least, that the right hand and left hand of the DOJ do not know what the other is doing. The obvious ramifications of this matter require objective and honest answers. Further, I would like this briefing to include an update on the outstanding investigation into whom at the DOJ and/or FBI leaked information to the press regarding the investigation of Dr. Steven Hatfill. As you are well aware, this investigation into the leak to the media has been ongoing for a number of years and yet, no individuals have been publicly named or reprimanded. I find this particularly troubling given that the American taxpayers ultimately picked up the tab and paid Dr. Hatfill nearly \$6 million as a settlement in a civil case.

Thank you for your cooperation and attention to this important matter. I appreciate you scheduling this briefing with my staff as soon as possible.

Sincerely,



Charles E. Grassley
Ranking Member

PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
CHARLES F. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLOOMBERG, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
ORIN G. HATCH, UTAH
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TOM COBURN, OKLAHOMA

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

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

October 5, 2011

Via Electronic Communication

The Honorable Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Attorney General Holder:

On September 30, 2011, it was reported that Anwar al-Awlaqi was killed in an operation conducted by the United States in Yemen. According to media accounts, the operation was conducted following the issuance of a secret memorandum issued by the Department of Justice authorizing the targeted killing of a U.S. citizen abroad. The published accounts include details provided by "administration officials" and describe the memorandum as the product of a review of legal issues raised by targeting and killing a U.S. citizen.

As the Ranking Member of the Committee on the Judiciary, I request that you provide a copy of the memorandum described in press accounts to the Committee for review. This document should be made available, along with any other corresponding, related, or derivative memoranda that were prepared as part of drafting the memorandum. The memorandum should be made available in an unredacted manner. Should the memorandum be classified, please alert my staff so appropriate procedures can be followed to transmit the document.

Thank you for your cooperation and attention to this important matter. I would appreciate your response, including the requested memorandum, no later than October 21, 2011.

Sincerely,



Charles E. Grassley
Ranking Member

PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN
 DIANNE FEINSTEIN, CALIFORNIA
 CHARLES E. SCHUMER, NEW YORK
 RICHARD J. DURBIN, ILLINOIS
 SHELDON WHITEHOUSE, RHODE ISLAND
 AMY KLOBUCHAR, MINNESOTA
 AL FRANKEN, MINNESOTA
 CHRISTOPHER A. COONS, DELAWARE
 RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
 ORRIN G. HATCH, UTAH
 JON KYL, ARIZONA
 JEFF SESSIONS, ALABAMA
 LINDSEY O. GRAHAM, SOUTH CAROLINA
 JOHN CORNYN, TEXAS
 MICHAEL S. LEE, UTAH
 TOM COBURN, OKLAHOMA

United States Senate

COMMITTEE ON THE JUDICIARY
 WASHINGTON, DC 20510-6275

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

November 14, 2011

Via Electronic Transmission

The Honorable Eric H. Holder
 Attorney General
 U.S. Department of Justice
 950 Pennsylvania Avenue, N.W.
 Washington, DC 20530

Dear Attorney General Holder:

I write to express my concerns regarding the perpetual delays for resolving Federal Bureau of Investigation (FBI) whistleblower cases at the Department of Justice (DOJ). As you are well aware, I am a long-standing advocate for whistleblower rights. Whistleblowers point out fraud, waste, and abuse when no one else will, and they do so while risking their professional careers. Whistleblowers have played a critical role in exposing failed government operations such as Operation Fast and Furious, and retaliation against whistleblowers should never be tolerated. Thus, I am concerned about the treatment of whistleblowers at the FBI, specifically in the cases of Jane Turner and Robert Kobus. The process of resolving whistleblower claims appears to be broken.

Jane Turner was a career FBI agent with an outstanding record for conducting investigations involving missing and exploited children. Agent Turner filed a whistleblower complaint with the Department of Justice, Office of the Inspector General (OIG), in 2002 when she discovered that FBI agents removed items from Ground Zero following the terrorist attacks of 9/11. Unfortunately, Agent Turner was forced to file an appeal to the Office of Attorney Recruitment and Management (OARM) due to the OIG's delayed decision in their investigation. Ultimately, the OARM substantiated her allegations in May, 2010, and the FBI was ordered to provide Agent Turner back pay, attorney's fees, and other relief. It is my understanding that the FBI filed an appeal to the Deputy Attorney General concerning the issue of back pay, despite the FBI's failure to raise the issue of back pay during previous OARM proceedings, and the case was remanded, in part, back to OARM for further review of the back pay issue. Consequently, a final resolution to Jane Turner's reprisal case against the FBI is now further delayed by the Deputy Attorney General's curious decision. Given the already excessive delays in this case, the ruling by the Deputy Attorney General postpones a judgment that should have come much sooner. I remind you that Agent Turner initially filed her complaint approximately 9 years ago, and she has yet to receive a final decision. Any reasonable person would agree that 9 years is extreme and unacceptable.

Robert Kobus is a 30 year non-agent employee of the FBI who disclosed time and attendance fraud by FBI agents. The OIG also conducted an investigation into these allegations and substantiated that he was retaliated against for protected whistleblowing. The FBI management not only demoted Mr. Kobus to a non-supervisory position, but they even went so far as to move him from his office to a cubicle on the vacant 24th floor of the FBI's office building. Nevertheless, the OIG's findings were referred to OARM for adjudication and Mr. Kobus' case has now languished in bureaucratic red tape for approximately 4 years.

I'm confident you would agree that a cumulative 13 years is an excessive amount of time to complete two whistleblower investigations. You previously stated during your testimony to the Senate Judiciary Committee that you will "ensure that people are given the opportunity to blow the whistle and they will not be retaliated against, and then to hold accountable anybody who would attempt to do that."¹ You also stated that, "I have seen their [whistleblowers'] utility, their worth, and, frankly, the amount of money that they return to the Federal Government. And they serve a very, very useful purpose."² The Deputy Attorney General, in his responses to congressional "Questions for the Record", asserted he would "work with the Judiciary Committee and the independent Office of Special Counsel, which investigates and prosecutes violation of law, including reprisals against whistleblowers, to provide timely and accurate information to the Congress."³ He further pledged he would "not tolerate unlawful retaliation against any Department of Justice employee, including FBI employees" and he would "work to ensure that there are adequate safeguards so that whistleblowers receive all of the protections to which they are entitled by law."⁴ I would ask that you honor these statements and ensure these cases, and others like them, are investigated and decided in a reasonable timeframe.

Given your previously stated support for whistleblowers, I presume that you would agree that DOJ is sending the wrong message to whistleblowers by taking an inordinate amount of time to issue final declarations for Agent Turner and Mr. Kobus. The excessive time the OARM has taken to issue a final judgment, which is further exacerbated by the Deputy Attorney General's recent decision in Agent Turner's case, has cast your department in a dubious light regarding your stated support for whistleblowers. These excessive delays indicate that the process of adjudicating a FBI whistleblower claim is broken. Consequently, I ask that you review these matters and ensure that the OARM and the Deputy Attorney General conduct their respective reviews in a transparent and expeditious manner. While I appreciate that allegations of fraud, waste, and abuse must be properly investigated, Agent Turner and Mr. Kobus deserve transparency in the process and finality to their cases.

Thank you for your cooperation and attention to this important matter. I request you provide a written response to this letter no later than November 21, 2011.

¹ Committee on the Judiciary, United States Senate, Nomination of Eric H. Holder, Jr., Nominee to be Attorney General of the United States, January 15 & 16, 2009

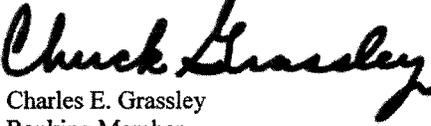
² *Id.*

³ Responses to Questions for the Record of the June 15, 2010 Confirmation Hearing of James M. Cole, Nominee to be Deputy Attorney General

⁴ *Id.*

79

Sincerely,


Charles E. Grassley
Ranking Member

Cc: The Honorable Patrick Leahy
Chairman

**STATEMENT OF SENATOR PATRICK LEAHY (D-VT.),
CHAIRMAN, SENATE JUDICIARY COMMITTEE
HEARING ON OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION
DECEMBER 14, 2011**

Today the Judiciary Committee hears from Director Robert Mueller of the Federal Bureau of Investigation. This is the Director's third appearance before this Committee this year.

I thank Director Mueller once again for agreeing to put his life on hold when called upon by the President earlier this year to continue to serve as FBI Director. His commitment and dedication to service are exemplary.

The Bureau plays an integral role in protecting our Nation's security through its counterterrorism investigations and intelligence gathering. Its work has contributed to more than 400 convictions in terrorism cases since September 11, 2011. Knowing this, I remain deeply concerned about a provision of the National Defense Authorization bill that would mandate—mandate—the military detention of certain terrorism suspects, even if they are arrested on U.S. soil.

Director Mueller has written that this provision would adversely impact the Bureau's ability to conduct counterterrorism investigations and inject "a substantial element of uncertainty" into its operations. I appreciate what Director Mueller meant when he wrote that the misguided provision fails to take into account "the reality of a counterterrorism investigation."

Congress needs to do more to support important law enforcement efforts. We should give law enforcement the appropriate tools to combat the growing threat of cybercrime. More and more, American consumers and businesses are being targeted by sophisticated cyberattacks designed to steal their most sensitive information. In September, this Committee again voted for the Personal Data Privacy and Security Act, S.1151, which is long overdue legislation that will provide tools to help law enforcement combat cybercrime. The Senate and the Congress should promptly pass this measure.

In the last Congress, we made great strides toward more effective fraud prevention and enforcement. I worked hard with Senators on both sides of the aisle to craft and pass the Fraud Enforcement and Recovery Act, the most expansive anti-fraud legislation in more than a decade. We enacted important anti-fraud provisions as well as part of both healthcare and Wall Street reform legislation. I am pleased to see that the FBI has greatly increased the number of agents investigating fraud, leading to more fraud arrests and greater fraud recoveries.

This year, I introduced the Fighting Fraud to Protect Taxpayers Act, which redirects a portion of the fines and penalties collected from wrongdoers back into fraud enforcement efforts. This bill would lead to substantial recoveries, paying for itself many times over. This Committee voted for the bill more than six months ago. The Senate and Congress should pass this bill without further delay to give law enforcement the resources and tools they need to crack down on fraud.

I commend the FBI for also maintaining its historic focus on combating corruption. I have worked to develop bipartisan, bicameral anti-corruption legislation, the Public Corruption

Prosecution Improvements Act. I have also worked on the Civilian Extraterritorial Jurisdiction Act, which would hold accountable American contractors and employees abroad who engage in corruption and contracting fraud. At a time when anger at corporate wrongdoing, greed, and corruption is at an all-time high, Congress should act promptly to give the FBI and other Federal law enforcement the tools they need to reign in fraud and corruption. These measures have been sent by this Committee to the Senate. The Senate and the Congress should pass the Public Corruption Prosecution Improvements Act, S.401, and the Civilian Extraterritorial Jurisdiction Act, S.1145.

In each of these matters, we should not let partisanship get in the way of helping law enforcement agencies do their jobs as effectively as possible. Too often these days, whether it is Senator Whitehouse's bill, S.1793, to make sure the FBI can respond to requests from local officials to provide help investigate violence crimes, Senator Blumenthal's bill, S.1794, to close a gap in the law with respect to the authority of the Secret Service, or our bill, S.1792, to ensure that the U.S. Marshals upon request can provide timely assistance in missing children cases, obvious measures are being delayed for no good purpose. I wish we all respected our law enforcement and national security agencies more and gave them the support they need and deserve. Instead, too many seem interested in tearing them down and undermining them at all levels.

I thank Director Mueller for returning to the Committee, for working with us, and for his responsiveness to our oversight efforts. Through him I thank the hardworking men and women of the FBI who do vital work every day to help keep us safe.

#####



Department of Justice

STATEMENT OF
ROBERT S. MUELLER III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON JUDICIARY
UNITED STATES SENATE

REGARDING
OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

PRESENTED
DECEMBER 14, 2011

**STATEMENT FOR THE RECORD OF
ROBERT S. MUELLER III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
AT A HEARING ENTITLED
OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION
PRESENTED
DECEMBER 14, 2011**

Introduction

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

Three months ago, our nation marked the tenth anniversary of the September 11th attacks. The horrific events of that day were the prelude to a decade of political, economic, and cultural transformation. Since that time, there have been significant changes in political leadership around the world, including the recent events in Libya and Egypt. In the economic arena, the past decade has seen billion dollar investment frauds, the failure of storied financial institutions, and the abuse of financial vehicles such as credit default swaps and mortgage backed securities which have undermined the world's financial system. There has also been an exponential rise in the proliferation of new technologies, and these advancements have changed the way we work, socialize and communicate with one another.

These changes in the global landscape have posed significant challenges to members of law enforcement and the Intelligence Community. Accelerated by these changes, the threats to our nation are constantly evolving, and today's FBI now faces a more complex threat environment than ever before.

Since 9/11, the FBI has shifted to be an intelligence-driven, threat-focused organization, guided by clear operational strategies. The FBI is focused on predicting and preventing the threats we face while engaging the communities we serve. This shift has led to a greater reliance on technology, collaboration with new partners, and human capital. The FBI is a full member of the U.S. intelligence community, and serves as a critical link between the intelligence and law enforcement communities in the United States. The FBI, as an organization, is in a unique position to address national security and criminal threats that are increasingly intertwined.

Counterterrorism

Al Qaeda and its affiliates and adherents continue to present the most significant threat to our national security. Despite the coordinated efforts of our military, Intelligence Community, law enforcement and international partners, core Al Qaeda, operating out of Pakistan, remains committed to high profile attacks against the United States. These efforts have been confirmed by intelligence seized from Osama Bin Laden's compound upon his death.

In addition, Al Qaeda affiliates such as Al Qaeda in the Arabian Peninsula (AQAP) have emerged as significant threats to our nation. These groups have attempted several attacks against the homeland and our citizens and interests abroad, including the failed Christmas Day airline bombing in 2009 and the attempted bombing of U.S.-bound cargo planes in October 2010.

Apart from its physical presence, Al Qaeda's online presence has become a significant additional concern over the past ten years. Al Qaeda has used the Internet as a far reaching tool to recruit and radicalize followers, and to incite acts of terrorism. Homegrown violent extremists often communicate with like-minded individuals online. They are individuals without a typical profile, are increasingly savvy, and are willing to act alone. As such, homegrown violent extremists are among the most difficult to detect and stop.

An example of the danger posed by self radicalized individuals is that of Rezwan Ferdaus, a 26 year old U.S. citizen and graduate student living in Boston, Massachusetts. This fall, Ferdaus allegedly planned to use unmanned, remote-controlled aircraft to attack locations in Washington, D.C., including the Capitol. Ferdaus was influenced by online anti-American speech, among other things, and had expressed admiration for al Qaeda's leaders, but was not directly affiliated with any group or other would-be terrorists. He had allegedly become radicalized on his own, making his activities much more difficult to detect. Ferdaus is currently awaiting trial in the United States District Court for the District of Massachusetts.

Recent cases exemplify the need for the FBI to continue to enhance our intelligence capabilities to get critical information to the right people at the right time – *before* any harm is done.

The foundation for the FBI's success against terrorism over the past ten years has been strong partnerships and the ability to collect, analyze and disseminate intelligence. In compliance with the law, the FBI collects, exploits and disseminates intelligence to a greater and more useful extent now than it has ever before. This focus on intelligence has helped us prioritize our top threats and increase our understanding of our vulnerabilities to these threats.

Counterintelligence

While foreign intelligence services continue traditional efforts to target political and military intelligence, more modern counterintelligence threats include efforts to obtain technologies and trade secrets from corporations and universities. The loss of critical research and development data, intellectual property, and insider information continues to pose a significant threat to national security.

For example, this past January, Noshir Gowadia was sentenced to 32 years in prison for offering classified knowledge of military design techniques to foreign nations. For 18 years, Gowadia had worked as an engineer at Northrop Grumman, the defense contractor that built the B-2 stealth bomber. Beginning in 1995, Gowadia offered his classified knowledge regarding achieving stealth in military aircraft to foreign nations willing to pay for it. Over the course of ten years, Gowadia traveled to foreign countries, including six trips to China, to assist in the military application of stealth techniques derived from his work on the B-2 bomber.

Last month, Kexue Huang, a former scientist for two of America's largest agriculture companies, pled guilty to charges that he sent trade secrets to China. While working at Dow AgriSciences and later at Cargill, Huang became a research leader in biotechnology and the development of organic pesticides. Although he had signed non-disclosure agreements, he transferred stolen trade secrets from both companies to persons in Germany and China, causing great economic harm to Dow and Cargill.

These cases illustrate the growing scope of the "insider threat" from employees who use their legitimate access to steal secrets for the benefit of another company or country. Through our relationships with businesses, academia, and U.S. government agencies, the FBI and its counterintelligence partners must continue our efforts to identify and protect sensitive American technology and projects of great importance to the United States government.

Cyber Intrusions

The potential for relative anonymity on the Internet makes it difficult to discern the identity, motives, and location of intruders who seek to exploit our reliance on networked technologies. Further, the proliferation of portable devices that connect to the Internet only increases the opportunity to steal vital information. Since 2002, the FBI has seen an 84% increase in the number of computer intrusions investigations opened. The FBI cannot merely react to computer intrusions. Hackers will seek to exploit every vulnerability, and we must be able to anticipate their moves.

To actively pursue each of these threats, the FBI utilizes cyber squads in each of our 56 field offices. We have more than 1,000 specially trained agents, analysts, and digital forensic examiners that run complex undercover operations and examine digital evidence. The FBI is the Executive Agency for the National Cyber Investigative Joint Task Force.

Together, we analyze and share intelligence to identify key players and schemes and use our tools to disrupt significant cyber threats.

Our partnerships and joint initiatives in the cyber arena have been productive, especially in the national security realm. In 2010, the FBI strengthened our efforts to counter state-sponsored cyber threats, increasing the number of national security intrusion cases by 60%. While we increased our emphasis on national security, we continued to obtain results in matters involving criminal intrusions. In 2010, we arrested a record 202 individuals for criminal intrusions, up from 159 in 2009. Those arrests included five of the world's top cyber criminals. Among them were the perpetrators of the Royal Bank of Scotland (RBS) WorldPay intrusion. In addition, as a result of our strong partnership on cyber matters with the Estonian government, we have successfully extradited one of the first hackers from Estonia to the United States.

In April of this year, the FBI brought down an international "botnet" known as Coreflood. Botnets are networks of virus-infected computers controlled remotely by an attacker. To shut down Coreflood, the FBI took control of five servers the hackers had used to infect some two million computers with malware. In an unprecedented step, after obtaining court approval, we responded to the signals sent from the infected computers in the United States, and sent a command that stopped the malware, preventing harm to hundreds of thousands of users.

Just last month, the FBI and NASA's Office of Inspector General worked with partners throughout the world to take down a cyber criminal network operated by Estonian company Rove Digital. Seven individuals were charged with engaging in a scheme that spanned over 100 countries and infected four million computers. At least 500,000 of the victim computers were in the United States, including computers belonging to U.S. government agencies, educational institutions, non-profit organizations, commercial businesses, and individuals. We seized computers at various locations, froze the defendants' financial accounts, and disabled their network of US-based computers – including dozens of rogue Domain Name System (DNS) servers. In addition, we ensured that the defendants' rogue servers were immediately replaced with legitimate ones to minimize Internet service disruptions to users with malware infected computers. These complex and sophisticated cases demonstrate the FBI's ability to work effectively with our partners to combat this increasingly transnational crime problem.

Financial Crimes

Ten years ago, few were familiar with the names Raj Rajaratnam, Bernie Madoff, or Lee Farkas. Today, they remain symbols of unprecedented greed, whose egregious crimes have threatened the stability of our financial system and victimized countless taxpayers, homeowners, shareholders, and everyday citizens.

Corporate and Securities Fraud

The FBI and its law enforcement partners continue to uncover major frauds, insider trading activity, and Ponzi schemes. At the end of FY 2011, the FBI had more than 2,500

active corporate and securities fraud investigations, representing a 47% increase since FY 2008. Over the past three years, the FBI has obtained approximately \$23.5 billion in recoveries, fines and restitutions in such programs, and during FY 2011, the FBI obtained 611 convictions, an historic high. The FBI is pursuing those who commit fraud at every level, and is working to ensure that those who played a role in the recent financial crisis are brought to justice.

For example, in July 2011, former Taylor, Bean, and Whitaker (TBW) chairman Lee Farkas was sentenced to 30 years imprisonment for his role in a \$2.9 billion fraud that contributed to the failure of Colonial Bank, one of the 25 largest banks in the United States and the sixth largest bank failure in the country. In addition, six high-level executives and employees of TBW and Colonial Bank pleaded guilty, testified against Farkas, and were sentenced to prison time. For example, on June 17, 2011, Catherine Kissick, a former senior vice president of Colonial Bank and head of its mortgage warehouse lending division, was sentenced to eight years imprisonment for her role in that scheme.

In May 2011, Raj Rajaratnam, the founder of the Galleon Group hedge fund was convicted by a federal jury on all 14 counts pertaining to his insider trading activity. Rajaratnam was subsequently sentenced to 11 years in prison. The wide ranging probe into illicit insider trading activity on Wall Street and in boardrooms across the United States was conducted by the United States Attorney's Office for the Southern District of New York and the FBI's New York Field Office. To date, a total of 51 individuals have been charged, and 49 convictions have been obtained. Cases against the two remaining defendants are currently pending.

Health Care Fraud

The focus on health care fraud is no less important. The federal government spends hundreds of billions of dollars every year to fund Medicare and other government health care programs. In 2011, the FBI had approximately 2,664 active health care fraud investigations, up approximately 7% since 2009. Together with attorneys at the Department of Justice and our partners at the Department of Health and Human Services, the FBI is aggressively pursuing, fraud and abuse within our nation's health care system.

For example, in September 2011, the Medicare Fraud Strike Force—a partnership between the Department of Justice and the Department of Health and Human Services—charged more than 91 defendants in eight cities, including doctors, nurses, and other medical professionals, for their alleged participation in Medicare fraud schemes involving more than \$295 million in false billing. This coordinated takedown involved the highest amount of false Medicare billings in a single takedown in Strike Force history.

Also in September of this year, Lawrence Duran and Marianella Valera, the owners of a mental health care company, American Therapeutic Corporation (ATC), were sentenced to 50 and 35 years in prison, respectively, for orchestrating a \$205 million Medicare fraud scheme.

Mortgage Fraud

Through our task forces and working groups across the country, the FBI and its partners continue efforts to pinpoint the most egregious offenders, identifying emerging trends before they flourish. In FY 2011, these efforts translated into roughly 3,000 pending mortgage fraud investigations—compared to approximately 700 investigations in 2005. Nearly 70 percent of the pending investigations involve losses of more than \$1 million.

Our mortgage fraud work has included prosecutions of senior executives, not just lower level employees. For example, earlier this year, Michael McGrath, former president and owner of U.S. Mortgage Corporation, formerly one of the largest private residential mortgage companies in New Jersey, was sentenced to 14 years in prison for his role in perpetrating a corporate fraud scheme involving the double selling of mortgage loans to Fannie Mae, which resulted in losses in excess of \$100 million.

Public Corruption

Ten years ago, many of us had not heard of Jack Abramoff, or Bob Ney. Today, they serve as reminders of the damage caused by corruption within our government.

In October of this year, for example, the FBI and its Organized Crime Drug Enforcement Task Force (OCDETF) partners arrested 51 individuals in Arkansas as part of *Operation Delta Blues*. Included in the arrests were five local police officers, accused of accepting bribes to watch over shipments of cocaine, crack cocaine, marijuana and methamphetamines that moved across state lines. The operation, which was the culmination of a four year long investigation, was orchestrated by 700 federal and state law enforcement officers.

Just last month, a former lieutenant with the New Orleans Police Department (NOPD), was sentenced for his role in a conspiracy to obstruct justice and for misprision of a felony, in connection with a federal investigation of two police-involved shootings that left two civilians dead and four others seriously wounded in the area of the Danziger Bridge in the days after Hurricane Katrina.

And last year, more than 700 agents were deployed to Puerto Rico to arrest 89 law enforcement officers and 44 others on drug and corruption charges as part of *Operation Guard Shack*, the largest police corruption investigation in the history of the FBI.

Along the Southwest Border, the FBI continues to dedicate resources to Border Corruption Task Forces (BCTFs). Working closely with our partners at DEA, ATF, DOS, and DHS, our 13 BCTFs share information with the Southwest Intelligence Group (SWIG), the El Paso Intelligence Center (EPIC), and Mexican legal attachés to both identify and disrupt Mexican drug trafficking organizations (DTOs) from utilizing and soliciting United States public officials to commit criminal activities.

We also continue to confront international contract corruption through the International Contract Corruption Task Force (ICCTF). The ICCTF has investigative jurisdiction for all fraud against the U.S. government where the illegal conduct occurred outside the

United States and involves United States persons or funds. Since 2004, the ICCTF has been extremely successful, conducting over 1,000 investigations and obtaining more than \$500 million in fines, restitution, forfeitures, and seizures. Through these investigative efforts, nearly 250 individuals have been charged, including civilian and military personnel, contractors, third country nationals, and others.

Gangs/Violent Crime

Similarly, we are working hard to protect our communities from the longstanding threats from gangs and violent crime. The FBI has Violent Crime, Violent Gang Safe Streets and Safe Trails Task Forces across the country. Through these task forces, we identify and target major groups operating as criminal enterprises. Much of our intelligence comes from our state, local, and tribal law enforcement partners, who know their communities inside and out. We are using enhanced surveillance and embedded sources to track these gangs and to identify emerging trends. By conducting these multi-subject and multi-jurisdictional investigations, the FBI can concentrate on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

Violence Along the Southwest Border

The escalating violence associated with drug trafficking in Mexico continues to be a significant concern for the FBI and our partners. Our multi-faceted approach relies heavily on the collection and sharing of intelligence, which is made possible and enhanced through the Southwest Intelligence Group (SWIG), the El Paso Intelligence Center (EPIC), OCDETF Fusion Center, and via the intelligence community. Guided by intelligence, the FBI and its federal law enforcement partners are working diligently, in coordination with the Government of Mexico, to stem the flow of illicit drugs into the United States. We are also cooperating closely with the Government of Mexico in their efforts to break the power and impunity of the drug cartels inside Mexico.

Most recently, the collective efforts of the FBI, DEA and our many U.S. and Mexican law enforcement partners have resulted in the identification and indictment of thirty-five leaders, members, and associates of one of the most brutal gangs operating along the U.S.-Mexico border on various counts of racketeering, murder, drug offenses, money laundering, and obstruction of justice. Of those 35 subjects, 10 Mexican nationals were specifically charged with the March 2010 murders in Juarez, Mexico of a U.S. Consulate employee and her husband, along with the husband of another consulate employee.

The FBI has achieved many operational successes along our borders by obtaining a cross-programmatic perspective of the multi-faceted threats we face. To address these complex threats we have developed "hybrid squads" consisting of multi-disciplinary teams of special agents, intelligence analysts, staff operations specialists, and other professionals. The diversity of experience in investigating matters ranging from gang activity, violent crime, and public corruption allows us to address border threats from multiple angles.

Organized Crime

Ten years ago, when we thought of organized crime, we thought of regional pockets of La Cosa Nostra. Today, those images have been replaced with images of international enterprises that run multi-national, multi-billion-dollar schemes from start to finish. Regional crime families with clear structures have been replaced with flat, fluid networks that have a more global reach. As noted by Attorney General Eric Holder last July at the roll out of the President's Transnational Organized Crime Strategy, "our efforts to prevent and combat transnational organized crime have never been more urgent." We continue to work with our federal, state, local, and international partners in the implementation of this strategy.

For example, late last year the FBI and its partners arrested and indicted over 70 members and associates of an Armenian organized crime ring for their role in nearly \$170 million in health care fraud crimes. This case, which involved more than 160 medical clinics, was the culmination of a national level, multi-agency, intelligence driven investigation. To date, it remains the largest Medicare fraud scheme ever committed by a single enterprise and criminally charged by the Department of Justice.

We are also expanding our efforts to include West African and Southeast Asian organized crime groups. We continue to share intelligence about criminal groups with our partners, and to combine resources and expertise to gain a full understanding of each group. In furtherance of these efforts, the FBI also continues to participate in the International Organized Crime Intelligence Operations Center. The IOC2, as it is known, is responsible for coordinating the efforts of nine federal law enforcement agencies in combating non drug transnational organized crime networks.

Crimes Against Children

Without question, the last decade has been one of unprecedented growth and change for our agency. While we have seen the emergence of many new threats, we also continue to work with our partners to continue protecting our communities from long enduring threats. For example, today's FBI remains vigilant in its efforts to remove predators from our communities and to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Through globalization, law enforcement also has the ability to quickly share information with partners the world over and our outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate parents and children about the dangers posed by violent predators and recover missing and endangered children who have been taken. Through our Child Abduction Rapid Deployment teams, Innocence Lost National Initiative, Innocent Images National Initiative, Office of Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to make the world a safer place for our children.

Indian Country

The FBI also maintains primary federal law enforcement authority for felony crimes in Indian Country. Even as demands persist across a broad threat spectrum, Indian Country

law enforcement remains a priority for the FBI. Last year, the FBI handled more than 2,400 Indian Country investigations throughout the nation.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Available statistics indicate that American Indians and Alaska natives suffer violent crime at far greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations involve homicide, crimes against children, or felony assaults. In addition, recent Congressional findings reveal that 34% of American Indian and Alaska Native women will be raped in their lifetimes, and that 39% will be the subjects of domestic violence. To address these threats, the FBI has deployed 9 new investigators to Indian Country as part of DOJ's broader effort to fight crime in tribal communities.

Addressing crimes against Native American women is a particular priority for the Administration. Since the President signed the Tribal Law and Order Act (TLOA) into law 2010, DOJ has taken several steps towards implementation of TLOA. Implementation of TLOA has resulted in partnerships between federal departments to address the needs of victims of sexual assault, and the FBI's Office of Victim Assistance is partnering with the Indian Health Service to expand and support Sexual Assault Nurse Examiner and Sexual Assault Response Team programs for Indian Country.

The gang threat on Indian reservations continues to be a concern for the FBI, as is gang-related violent crime. Currently, the FBI has 16 Safe Trails Task Forces focused on drugs, gangs, and violent crimes in Indian Country. In addition, the FBI continues its efforts to address the emerging threat from fraud and other white-collar crimes committed against tribally run gaming facilities.

Future Challenges

The FBI has always adapted to meet new threats. Together, with our partners, we must continue to evolve to address those who seek to threaten national security and to violate the laws of the United States.

Regardless of the nature of the emerging threat, the rule of law will remain the FBI's guiding principle, as will the protection of privacy and civil liberties for the American people. In June 2007, the FBI established its Integrity and Compliance Program to identify and mitigate legal compliance risks within the FBI. We are pleased that the Department of Justice's Office of the Inspector General (OIG) recently recognized that this program represents a fundamental change in how we evaluate and manage legal compliance risks. The OIG concluded that the program promotes the reporting of compliance concerns and has improved FBI management's knowledge of and response to such concerns. The OIG recommended that other agencies consider implementing a similar kind of program.

Other significant challenges posed to the FBI in the accomplishment of our diverse mission include those that result from the advent of rapidly changing technology. A growing gap exists between the statutory authority of law enforcement to intercept electronic communications pursuant to court order and our practical ability to intercept those communications.

Should this gap continue to grow, there is a very real risk of the government “going dark” resulting in an increased risk to national security and public safety. The Administration has convened an interagency working group to review this issue and identify possible solutions. Any proposed legislation will be appropriately coordinated through the interagency process and then raised with this Committee.

Conclusion

Chairman Leahy and Ranking Member Grassley, I would like to conclude by thanking you and this committee for your continued support of the FBI’s mission. I look forward to working with the Committee to improve the FBI as our transformation continues in the future. I would be happy to answer any question that you may have.

**U.S. Department of Justice**

Office of Legislative Affairs

*Assistant Attorney General**Washington, D.C. 20530*

August 8, 2011

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

Dear Senator Grassley:

This responds to your letters to the Attorney General dated May 16, 2011, and July 29, 2011 regarding a possible criminal investigation or prosecution of Ali Mussa Daqduq. We are sending an identical response to the other Members who joined in your letter to us.

As you know, Ali Mussa Daqduq is currently in United States military custody in Iraq and we refer you to the Department of Defense for information concerning his status. The ultimate disposition of this matter is under consideration by an interagency process that includes the Department of Defense, the Intelligence Community, the State Department, the Department of Homeland Security, and the Department of Justice.

The Department remains committed to using all available tools to fight terrorism, including prosecution in military commissions or Article III courts, as appropriate. The decision to utilize one tool versus another will be made by the members of the interagency review process based on the facts and the law, and guided by the national security interests of the United States.

In addition, you have asked about a July 2009 letter regarding Laith and Qais al Khazali. We understand that this letter was addressed to the White House, not to the Justice Department, but now that you have brought it to our attention we will assist in ensuring that an appropriate response is provided.

We appreciate your interest in this matter. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "m w", written over a light blue horizontal line.

Ronald Weich
Assistant Attorney General

cc: The Honorable Patrick J. Leahy
Chairman



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 23, 2011

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

Dear Senator Grassley:

This responds to your letter to the Attorney General and the Director of the Federal Bureau of Investigation, dated August 31, 2011, regarding the investigation of the 2001 anthrax letter attacks. We understand that you have concerns regarding recent developments in the wrongful death suit filed by the family of the first victim of the anthrax letter attacks, *Stevens v. United States*, pending in the Southern District of Florida.

You expressed concern that documents filed in the civil action "seemingly contradicted previous information provided to congressional leadership" and "indicated that the DOJ no longer believed that Dr. Ivins created refined anthrax powder in his laboratory." The motion for summary judgment filed by the Department's Civil Division in this litigation does not contradict the findings in the FBI criminal investigation. To the contrary, the Department has stated in defending the civil action "that the evidence would show that Dr. Ivins was the anthrax assailant." That statement was specifically recited no fewer than 15 times in the dispositive motion filed by the Department.

The issue raised by the United States in its motion did not pertain to whether Dr. Ivins was responsible for the anthrax attacks or whether he could have created the anthrax powder in his laboratory. The issue raised by our motion is whether the Army failed to properly oversee and supervise operations at the United States Army Medical Institute of Infectious Disease (USAMRIID) such that the agency was negligent in failing to anticipate and prevent the theft of liquid anthrax and its conversion into powder for use in the attacks. As stated in our motion and supporting documents, we believe that under applicable Florida tort law, the tragic death of Mr. Stevens from anthrax spores was not a "foreseeable" consequence of USAMRIID's anthrax research operations, given the unprecedented nature of the attacks, the substantial distance between the research and exposure, and the intervening transformation of laboratory material into the form used in the attacks.

The Honorable Charles E. Grassley
Page 2

As explained in our motion, in that limited respect, the transformation of the liquid anthrax (which was the form of viable anthrax used in research at the Army lab) into powdered form required a number of steps that were outside of USAMRIID's standard anthrax research practices. Also, in the higher biosafety level containment unit where researchers, including Dr. Ivins, had access to live anthrax in liquid form, there was no lyophilizer, specialized equipment that might have been used to dry the anthrax into powder. Accordingly, as the motion states, for proximate cause purposes under Florida law, it was not *foreseeable* to the Army at the time of the events alleged in the *Stevens* complaint that Dr. Ivins, or any other person employed at the facility, was in a position to accomplish such criminal acts. Nothing in that filing, however, is inconsistent with our conclusions that Dr. Ivins actually prepared the powdered anthrax that killed Mr. Stevens and that he did so at USAMRIID. While several of Dr. Ivins' former colleagues may have doubts about his ability to surreptitiously produce the anthrax powder in the specialized equipment available to him at the lab, we are convinced that he did so based upon the totality of the evidence developed in the criminal investigation, which has been previously briefed to the Senate Judiciary Committee. The doubts of his colleagues only underscore our view that Dr. Ivins' actions were not foreseeable under Florida tort law.

The Department's supplemental filing was not a retraction but a clarification that, although there was no lyophilizer available in the same BSL-3 containment unit where researchers had access to the liquid anthrax in the Army lab, there was a lyophilizer available in a BSL-2 containment unit in close proximity to the BSL-3 containment unit where the liquid anthrax was stored. That clarification was submitted both to ensure that the pleading was technically accurate, and also to counter a misconstruction of the government's motion that was reflected in the media at the time, suggesting that the Department had effectively contradicted its findings in the criminal investigation by contending in the civil case that it was "impossible" for Dr. Ivins to have produced the anthrax powder. No such assertion was made in the original or supplemental civil filing, which only identified the location of the lyophilizer as one of several elements that made the transformation of liquid anthrax to powdered form unforeseeable to USAMRIID officials, for tort law purposes. The court's decision to allow the government's supplemental filing, based upon a finding of "good cause," indicates a recognition that the Department sought only to clarify its prior filings, not to present contradictory theories.

It is also noteworthy that, even before the referenced motions were filed, the Department filed a motion in the civil action requesting, in substance, that the court require plaintiffs to acknowledge there had been no evidence presented in the case that would support a conclusion that anyone other than Dr. Ivins perpetrated the anthrax attacks. Any suggestion that the Department's position in the civil action has at any point conflicted with its earlier conclusions in the criminal investigation – that it would have proven Dr. Ivins's guilt beyond a reasonable doubt – is clearly rebutted by this record.

The Honorable Charles E. Grassley
Page 3

You also have asked about alleged leaks related to this investigation. After an extensive investigation, career prosecutors concluded that, based upon the Principles of Federal Prosecution, criminal charges were not appropriate in this matter. The Department does not identify individuals who may be the subject of internal deliberations regarding administrative action. Further, as you know, the Department settled a civil suit with Dr. Hatfill based on disclosures about him.

We hope this information is helpful and clarifies our position in this matter. In light of the pending litigation, it would be difficult for us to provide a briefing, but please let us know if you have additional questions. Please do not hesitate to contact this office if we may provide additional assistance regarding any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Weich", written in a cursive style.

Ronald Weich
Assistant Attorney General

cc: The Honorable Patrick J. Leahy
Chairman



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 30, 2011

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

Dear Senator Grassley:

This responds to your letter dated November 14, 2011, in which you express concern about delays in resolving FBI whistleblower reprisal cases. The Department shares your concerns and has recently implemented several changes to improve the effective and efficient adjudication of FBI whistleblower cases.

The time required for the Department's final resolution of an FBI whistleblower case is dependent upon a number of factors, including: the complexity of the legal and factual issues presented; the time for and extent of discovery; the time for the parties' respective briefs on the issues; the number and procedural posture of other such cases pending at one time; and whether the parties proceed to a hearing before the Director of the Office of Attorney Recruitment and Management (OARM), where the parties have the opportunity to call and cross-examine witnesses. In some instances, delay results from stay requests and requests for extension of the deadlines for discovery and submissions of briefs made by the parties. For example, in one of the cases you cite, a party asked for a stay to pursue a concurrent Title VII case. To allow the complainant/employee claiming retaliation the fairest opportunity to pursue redress, the Department has been very willing to grant such requests.

This is not to suggest that such requests are the sole or even most significant cause for delay. The legal requirements and various stages of review in adjudication of an FBI whistleblower case also affect case processing time. Before a complainant may file a request for corrective action with OARM, the complainant must first file a complaint of reprisal with either the Department's Office of Professional Responsibility (OPR) or Office of the Inspector General (OIG). The complainant may then file with OARM, but only within certain time requirements, *i.e.*, either within 60 calendar days of receipt of notification from the Conducting Office¹ that it is terminating its investigation, or any time after 120 calendar days from the date the complainant first filed the complaint of reprisal with the Conducting Office if the complainant has not been notified by the Conducting Office that it will seek corrective action. To enforce corrective action, the matter must be brought to OARM (*See* 28 C.F.R. § 27.3-27.4).

¹The term "Conducting Office" refers to whichever of OIG or OPR examines the initial complaint.

The Honorable Charles E. Grassley
Page 2

After filing with OARM, the complainant must establish jurisdiction over the claim by making a nonfrivolous allegation that the complainant made a protected disclosure that was a contributing factor in the FBI's decision to take, or fail to take (or threaten to take or fail to take), a personnel action. An employee who establishes jurisdiction, must then prove the merits of the allegations by preponderant evidence. If the employee meets that burden, OARM may order corrective action as appropriate and authorized by the regulations, unless the FBI proves by clear and convincing evidence that it would have taken the same personnel action in the absence of the employee's protected disclosure. As these are adversarial proceedings, the parties at each stage require time to present motions and written and/or oral arguments, and to conduct discovery. The parties have the opportunity to seek review of any final determination by the Deputy Attorney General.

As noted above, the Department has recently implemented several changes to significantly shorten the adjudication of FBI whistleblower cases. OARM has adopted a number of procedural guidelines modeled after those utilized by the administrative judges of the U.S. Merit Systems Protection Board to substantially reduce case processing time. A copy of OARM's case processing directive, effective October 14, 2011, is attached and can also be found on OARM's FBI whistleblower website at: <http://www.justice.gov/oarm/wb/whistleblowers.htm>.

The Department has also devoted additional resources to this task. While the current number of cases on OARM's docket is relatively small, the number of cases pending at one time fluctuates and can be heavily impacted by cases in which complex and novel factual and legal issues are presented, and where discovery is extensive and contentious. To expedite the resolution of pending cases, the Department has funded an attorney detail position to augment the staff conducting case reviews. A senior-level official from the U.S. Merit Systems Protection Board with extensive experience has filled the position. The Department will continue to closely monitor these changes to assess their impact on the process, and will make further adjustments as needed.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Ronald Weich
Assistant Attorney General

cc: The Honorable Patrick Leahy
Chairman