FEDERAL BUREAU OF INVESTIGATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MARCH 16, 2011

Serial No. 112–85

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

65–188 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

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM REED, New York
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
DEBBIE WASSERMAN SCHULTZ, Florida

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

CONTENTS

MARCH 16, 2011

FEDERAL BUREAU OF INVESTIGATION

WEDNESDAY, MARCH 16, 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to call, at 10:02 a.m., in room 2141, Rayburn Office Building, the Honorable Lamar Smith (Chairman of the Committee) presiding.

Present: Representatives Smith, Sensenbrenner, Coble, Gallegly, Chabot, Pence, King, Franks, Gohmert, Poe, Reed, Griffin, Marino, Gowdy, Ross, Adams, Quayle, Conyers, Scott, Watt, Jackson Lee, Waters, Quigley, Chu, Deutch, and Wasserman Schultz.

Staff present: (Majority) Sean McLaughlin, Chief of Staff and General Counsel; Allison Halataei, Deputy Chief of Staff/Parliamentarian; Crystal Jezierski, Counsel; Arthur Radford Baker, Counsel; (Minority) Perry Appelbaum, Staff Director and Chief Counsel; and Sam Sokol, Counsel.

Mr. SMITH. The Judiciary Committee will come to order.

Without objection, the Chair is authorized to declare recesses of the Committee at any time.

And we welcome everyone here today, Members, and particularly the Director of the FBI, Director Mueller, and we appreciate his willingness to testify today.

I am going to recognize myself for an opening statement, then recognize the Ranking Member for an opening statement.

Welcome, Director Mueller. I very much appreciate your being here today. Apparently this will be your last appearance before the House Judiciary Committee as FBI Director. We all thank you for your almost 10 years of dedicated public service.

Director Mueller began his tenure as FBI Director only days before the September 11th terrorist attacks. Since then, he has led the bureau through an ever-changing threat environment requiring a historic transformation of the agency.

Under his leadership, the FBI has successfully thwarted numerous terrorist plots, including plots to bomb New York's subway system, to destroy skyscrapers in Texas and Illinois, and to kill dozens of innocent Americans at a Christmas tree lighting ceremony in Oregon last December.

Terrorists remain intent on carrying out their plots to destroy America. Just last month, a 20-year-old student from Saudi Arabia was arrested in my home State of Texas for attempting to use weapons of mass destruction.

The terrorist threat may have changed, but it has not diminished. Our counter-terrorism laws must keep pace with the evolving threats.

It is imperative that Congress reauthorize the expiring provisions of the PATRIOT Act. Section 206 roving authority, section 215 business records, and the lone wolf definition are critical to apprehending terrorists before they strike.

Unfortunately, the myths surrounding the PATRIOT Act often overshadow the truth. As Congress considers the reauthorization of these provisions, we must set aside fiction and focus on the facts. These are key investigative tools of the FBI. The most recent example may be that section 215 business records authority was used to thwart last month's plot in Texas.

In the last decade, dramatic advances in technology have provided Americans with a wide variety of communication and research devices, but these new technologies have also enabled terrorists, spies, and criminals to operate with greater anonymity and less chance of detection.

As a result, our law enforcement agencies may increasingly find themselves in the dark. Simply put, the technical capability of law enforcement agencies needs to keep pace with new technologies.

Congress initially addressed this growing gap in 1994 when it passed legislation enabling law enforcement agents to conduct court-approved electronic surveillance. Since then, technology has continued to progress and we have new communication devices, new services, and new modes of communication. Yet, Federal law has not kept pace and does not address the contemporary challenge that law enforcement agencies face when attempting to intercept electronic communications.

"Going dark" is not about expanding the legal authority to conduct surveillance. It is about the inability to collect information that a judge has already authorized.

Congress must develop a solution that balances privacy interests, ensures continued innovation, and secures networks from unauthorized interceptions.

Technology also has facilitated a dramatic increase in the proliferation and exchange of child pornography. Child pornography was almost eradicated in America by the 1980's. Unfortunately, the Internet has reversed this accomplishment. Today pedophiles can purchase, view, or exchange this disturbing material with near impunity. In the last 12 years, electronic service providers have reported almost 8 million images and videos of sexually exploited children. Child pornography on the Internet may be our fastest growing crime, increasing an average of 150 percent a year. That must stop. Better data retention will assist law enforcement officers with the investigation of child pornography and other Internet-based crimes.

When investigators develop leads that might save a child or apprehend a pornographer, their efforts should not be frustrated because vital record were destroyed. Every piece of discarded information could be the footprint of a child predator.

I look forward to hearing from Director Mueller today on these and other issues of importance to the FBI and the country.

That concludes my opening statement.

And the gentleman from Michigan, the Ranking Member of the Judiciary Committee, is recognized for his opening statement.

Mr. CONYERS. Thank you, Chairman Smith.

Of course, top of the morning to our soon-to-be-departing-this-year Director Mueller.

We almost need a closed door session because some of the things we would like to talk about—well, maybe we might want to have one before you leave. It is not until September anyway.

The things that are uppermost in my mind are these. I would like to talk with you about your experiences here nearly a decade, and actually longer, in the FBI but as its leader nearly a decade. I am interested in how we can reduce gun violence in this country. I am deeply concerned about how we can more effectively control the drug epidemic in this country. And I am very interested in how we can improve and continue to improve our relations with the Muslim citizens in this country.

And so I look forward to your presentation and your review.

We have had a good relationship with the Federal Bureau of Investigation under your leadership. You have been available to us. We have been candid in our discussions across the years. Well, I guess it was a predecessor of yours that required that we put term limits on your job, but I join the Chairman in welcoming you here and I am sure all of the Members of the Judiciary Committee do as well.

Mr. SMITH. Thank you, Mr. Conyers.

Without objection, other Members' opening statements will be made a part of the record.

We are pleased to welcome today's witness, Robert S. Mueller, III, Director of the Federal Bureau of Investigation. Director Mueller was nominated by President George W. Bush and began his term as the sixth director of the FBI on September 4, 2001.

Director Mueller has a long and distinguished record of public service. Early in his career he served for 12 years as a prosecutor in the United States Attorney offices. After serving as a partner at the Boston law firm of Hill and Barlow, Director Mueller returned to the Justice Department in 1989, serving first as an assistant to the Attorney General. The following year, he took charge of its Criminal Division.

In 1998, Director Mueller was named United States Attorney in San Francisco, and he held that position until 2001.

Director Mueller is a graduate of Princeton University, earned his Master's degree at New York University and his law degree from the University of Virginia School of law.

He is also a decorated Marine, having received the Bronze Star, two Navy commendation medals, the Purple Heart, and the Vietnamese Cross of Gallantry.

The witness's written statement will be made a part of the record in its entirety, and Director Mueller, once again, we welcome you today and look forward to your statement.

TESTIMONY OF THE HONORABLE ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. MUELLER. Good morning to you, Chairman Smith, Ranking Member Conyers, and Members of the Committee. And I thank you for the opportunity to appear here today before you.

Today the Bureau faces unprecedented and increasingly complex challenges. We must identify and stop terrorists before they launch attacks against our citizens. We must protect our Government, businesses, and critical infrastructure from espionage and from the potentially devastating impact of cyber-based attacks. We must root out public corruption by white-collar crime, organized crime, stop child predators, and protect civil rights. We must also ensure that we are building a structure that will carry the FBI into the future by continuing to enhance our intelligence capabilities, improve our business practices and training, and develop the next generation of Bureau leaders. We must do all of this while respecting the authority given to us under the Constitution, upholding civil liberties and the rule of law.

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

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

In addition, there were a number of serious terrorist plots by lone offenders. Their targets ranged from a Martin Luther King Day march in Spokane, Washington to a Christmas tree lighting ceremony in Portland, Oregon to subway stations in Washington, D.C., and motives and methods of these plots, although varied, make these some of the most difficult threats to combat.

The espionage threat persisted as well. Last summer, there were the arrests of 10 Russian spies known as illegals who secretly blended into American society in order to clandestinely gather information for Russia.

And we continue to make significant arrests for economic espionage as foreign interests seek to steal controlled technologies. The cyber intrusion at Google last year highlighted the potential danger from a sophisticated Internet attack. Along with the countless other cyber incidents, these attacks threatened to undermine the integrity of the Internet and to victimize the businesses and people who rely on it.

In our criminal investigations, we continue to uncover billion dollar corporate and mortgage frauds that weaken the financial system and victimize investors, homeowners, and ultimately taxpayers.

We also exposed health care scams involving false billings and fake treatments that endangered patients and fleeced Government health care programs.

The extreme violence across our southwest border continues to impact the United States, as we saw the murders last March of American consulate workers in Juarez, Mexico and the shooting last month of two U.S. Immigration and Customs Enforcement agents in Mexico.

And throughout the year, there were numerous corruption cases that undermined the public trust and countless violent gang cases that continue to take innocent lives and endanger our communities.

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

Let me briefly discuss two areas where Congress could help the FBI with its mission.

First, we do encourage Congress to reauthorize the three FISA tools that are due to expire later this spring. The roving intercept authority is necessary for our national security mission and provides us with tools similar to what we use in criminal cases already. The business records authority permits us to obtain key documents and data in our national security cases, including our most serious terrorism matters. And the lone wolf provision is important to combat the growing threat from lone offenders and homegrown radicalization. These authorities, all of which are conducted with full court review and approval, are critical to our national security.

Second, the FBI and other Government agencies, as the Chairman alluded to, are now facing a growing gap in our ability to execute court-approved intercepts of certain modern communications technologies. We call this the problem of "going dark." With the acceleration of new Internet-based technologies, we are increasingly unable to collect valuable information and evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage. Let me emphasize that collecting this evidence has been approved by a court. But because the laws have not kept pace with changes in technology, we often cannot obtain the information responsive to the court order. And we look forward to working on this issue with this Committee and with Congress in the future months.

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

The support from this Committee and Congress has been an important part of transforming the FBI into the national security agency it is today. But for our transformation to be complete, we must continue to hire, train, and develop the best, brightest agents, analysts, and staff to meet the complex threats we face now and in the future. Under the current levels in the continuing resolution, the Bureau will have to absorb over $200 million in cuts, and without any changes, the current CR will leave us with over 1,100 vacant positions by the end of the year. And put simply, these cuts would undermine our efforts to transform the FBI and potentially to carry out our mission.

I appreciate the opportunity to review the FBI's recent work in responding to the far-reaching threats we face today, and I also want to thank the Committee for your continued support on behalf of the men and women at the FBI. And of course, I will be happy

to answer any questions you might have. Thank you, Mr. Chairman.

[The prepared statement of Mr. Mueller follows:]

Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

MARCH 16, 2011

STATEMENT FOR THE RECORD OF
ROBERT S. MUELLER, III
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES
AT A HEARING ENTITLED
"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"
PRESENTED
MARCH 16, 2011

I. Introduction

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

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

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

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

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

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

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

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

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

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

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

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

II. Counterterrorism

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

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

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

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

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

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

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

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

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

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

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

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

III. Cyber Security

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

Cyber Threats

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

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

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

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

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

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

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

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

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

Innocent Images National Initiative

The Innocent Images National Initiative (IINI), a component of the FBI's Cyber Crime Program, is an intelligence-driven, multi-agency operation combating the proliferation of online child pornography and child exploitation. The mission of the IINI is to reduce the vulnerability of children to acts of sexual exploitation and abuse facilitated through computers; to identify and rescue child victims; to investigate and prosecute sexual predators who use the Internet to exploit children for personal or financial gain; and to strengthen the capabilities of federal, state, local, and international law enforcement through training and investigative assistance.

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

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

One such investigation, dubbed Operation Achilles, involved our partners in Australia, New Zealand, Canada, Belgium, Italy, and Britain. The three-year investigation uncovered suspects who traded more than 400,000 images of children, many depicting acts of violence and

torture. Forty children were rescued, four websites were shut down, and 22 members of the ring were arrested. Fourteen of the 22 members were Americans who were successfully prosecuted by the Justice Department's Child Exploitation and Obscenity Section (Criminal Division) and the U.S. Attorney's Office for the Northern District of Florida.

Internet Fraud

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

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

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

IV. Counterintelligence

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

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

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

The FBI began a review more than a year ago, not related to WikiLeaks events, of information and network access policies through its Information Sharing Policy Board, to better balance policies governing the "need to know" with the "responsibility to share." We wanted to

ensure that FBI policy enabled appropriate internal and external sharing, and that statutory and Department of Justice guidance was applied throughout the FBI.

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

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

V. Criminal Programs

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

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

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

Mortgage Fraud

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

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

Health Care Fraud

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

Together with our partners in the Department of Justice and the Department of Health and Human Services, the FBI is fighting back. In FY2010, we recovered a record $4 billion on behalf of taxpayers. This represents an approximate $1.47 billion, or 57 percent, increase over the amount recovered in FY2009, which was itself a record amount. Indeed, over the past three years, we have collectively recovered an average of nearly $7 for every dollar expended. In FY2010, the Department of Justice brought criminal health care fraud charges against 931 defendants, the most ever in a single fiscal year, and we obtained 726 convictions, also a record. And the FBI continues to investigate nearly 2,600 cases of health care fraud.

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

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

Corporate Fraud

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

In December 2010, President Obama's interagency Financial Fraud Enforcement Task Force (FFETF) announced the results of Operation Broken Trust, which highlighted the prevalence of a wide range of investment fraud schemes around the country during a three-and-

a-half month period. This enforcement effort included investigations with hundreds of defendants who committed fraud schemes involving more than 120,000 victims and estimated losses totaling more than $8 billion.

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

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

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

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

Public Corruption

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

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

The FBI is also working to confront international contract corruption. The FBI's Criminal Investigative Division joined with our federal law enforcement partners to stand up the

International Contract Corruption Task Force (ICCTF), which includes all fraud against the U.S. government where the illegal conduct occurred outside the United States and involves United States persons or funds. Since 2004, the ICCTF has initiated nearly 800 investigations in Afghanistan, Iraq, and Kuwait.

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

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

Gang Violence

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

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

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

Organized Crime

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

But we have seen a shift from regional families with clear structures to flat, fluid networks with global reach. These international enterprises are running multi-national, multi-billion dollar schemes from start to finish. In an October 13, 2010, health care fraud takedown, 73 members and associates of organized crime groups (for example, Mirzoyan-Terdjanian Organization) were among those indicted for more than $163 million in health care fraud crimes. Among the defendants charged is Armen Kazarian, who is alleged to be a "Vory-V-Zakone," a term translated as "Thief-in-Law" and referring to a member of a select group of high-level criminals from Russia and the countries previously part of the former Soviet Union, including Armenia.

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

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

Violence and Corruption Along the Southwest Border

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

- Between 18 and 39 billion dollars flow annually from the United States across the Southwest Border to enrich the Mexican drug cartels.

- Over 3,000 drug-related murders in Juarez, Mexico, in 2010.

- Over 34,600 drug-related murders in all of Mexico from December 2006 to December 2010.

- Estimated that 95 percent of all South American cocaine that moves from South America to the United States goes through Mexico.

- 701,000 kilograms of marijuana were seized during the first five months of 2010 in Arizona, California, New Mexico, and Texas.

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

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

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

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

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

The FBI has been working closely with DHS in a joint effort to investigate the attack against two ICE special agents in Mexico on February 15, 2011, by suspected members of a Mexican drug trafficking organization. Jaime Zapata and Victor Avila were ambushed while traveling from Matehuala, Mexico, to Mexico City in an armored vehicle with diplomatic license

plates. Agent Zapata was killed in the attack. The Department of Justice created a joint task force to investigate these shootings, with the FBI as the lead task force agency. On February 24, 2011, Mexican law enforcement detained six individuals in connection with the shooting.

Crimes Against Children

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

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

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

To date, the ILNI has resulted in more than 600 federal and state convictions and the location and recovery of more than 1,300 children. Together, we have obtained substantial sentences for those convicted, including six life sentences and numerous others ranging from 25-45 years.

Indian Country

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

Approximately 75 percent of all FBI Indian Country investigations involve homicide, crimes against children, or felony assaults. Available statistics indicate that American Indians and Alaska Natives suffer violent crime at far greater rates than other Americans. Violence against Native women and children is a particular problem, with some counties facing murder rates against Native women well over 10 times the national average.[1] In addition to violence,

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

there is a significant emerging threat from fraud and other white-collar crimes committed against tribally run gaming facilities.

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

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

Information Technology

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

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

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

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

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

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

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

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

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

Conclusion

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

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

Mr. SMITH. Thank you, Director Mueller.

I will recognize myself for initial questions.

My first one, Director Mueller, goes to the need and importance of data retention by Internet service providers. There are a large number of Internet-based crimes today, particularly child pornography. I think probably the fastest growing crimes in America

today are identity theft and child pornography which, as I mentioned in my opening statement, is increasing at about 150 percent a year, as it has been for the last 15 years.

Would you let us know how you think better and perhaps longer data retention might be helpful to addressing some of those kinds of crimes?

Mr. MUELLER. Well, a number of years ago, for instance, when it comes to communications, telephone companies were the only means of communications. Records were kept by the telephone companies principally for billing purposes, and they were readily accessible in response to court orders requesting those records. With all the electronic communications in this day and age and companies that provide services that are not primarily communications providers, we have difficulty often in obtaining records from these particular companies. States in Europe, others, have a records retention statute that requires the retention of records for a period of time. We find in our investigations historical records are often, not in every case but I would say, historical records are important to our ability to develop an investigation to the point where we can arrest, indict, and hopefully convict that individuals who are responsible for the activity.

Mr. SMITH. Great.

Mr. MUELLER. I have talked about records retention in the past and am supportive of that form of legislation today.

Mr. SMITH. Thank you and that is helpful.

I would also like to ask you about the PATRIOT Act. You have told us why it is important, and I don't want to paint too bleak of a picture here, but what would happen if the three provisions that are due to expire, I think May 27th, are not made permanent? How would it hamper your investigations if we did not have those three provisions?

Mr. MUELLER. Let me start with the three provisions at issue. I will start with the business records provision. This enables us to go to the FISA Court, when we have a showing of relevance to an investigation, to obtain basic records that are necessary to provide predication for further investigation that are more intrusive, for instance, records from a WalMart, or in the case of Azazi where an individual is seeking to obtain hydrogen peroxide for an explosive device, we would want to get the records of those purchases. A person who goes to WalMart to buy components of an IED. We would want to get those records from WalMart.

Today we get those records in an international terrorism investigation by going to the FISA Court and with the 215 provision having the ability for the court to order the production of those records.

And it is not just those records I have identified. There are travel records. There are records relating to rental cars. All of these types of records are not covered by national security letters or covered by 215. We have used that provision over 380 times since 2001, and so it is an important provision.

The second one relates to roving wiretaps. Where we are able to show that an individual—it may be a foreign intelligence officer—is seeking to evade surveillance by buying throw-away cell phones in order to change cell phone activity on a daily basis, we are able

to go to the court under the current provisions and have the FISA Court direct that we are able to focus on that individual regardless of the particular cell phone that individual is using at a particular time. Otherwise, we have to go back to the court daily or weekly to get a re-up of those orders, and consequently, it is a great deal of additional manpower that would be required were we not to have the roving wiretap provision.

The other point I would say is on the criminal side of the house, we have had this for any number of years where we have the roving wiretap capability, and we have used it successfully on the criminal side and it makes no sense in my mind to have it on the criminal side but not on the national security side.

Lastly, the lone wolf provision was put into place to respond to the issue relating to Moussaoui, the individual who we believe back in advance of September 11 may have been here to be one of the pilots who was arrested by immigration services. The statute required that we show that he was affiliated with a particular terrorist group. We could not make that showing. We could not get the FISA order to look at his laptop. This provision was passed to address that particular incident. It is directed at non-U.S. citizens. It allows us to get a FISA warrant on an individual who is a terrorist but we cannot prove is affiliated with any particular group.

Mr. SMITH. Thank you, Director Mueller. I am going to squeeze in one more question. Maybe you can answer it very briefly.

Considering that we are in an unclassified setting, real quickly what do you think are the most urgent terrorist threats we face in America today? Is there a one, two, three?

Mr. MUELLER. I would say the top two are probably threats out of the FATA, out of Pakistan-Afghanistan border area from al-Qaeda. Shahzad, the Times Square bomber—and there have been a number of other individuals coming out of training in that particular area that have posed a threat and continue to pose a threat.

Secondly, and almost equal, is the threat from al-Qaeda in the Arabian Peninsula where you have seen the Christmas Day bombing of the year-plus ago, the attempt to come into Detroit and blow up the plane, as well as the two printers that were picked up in Dubai and in the UK recently. They were on their way to the United States and, if they had not been intercepted, would have blown up those planes.

Mr. SMITH. Okay.

Mr. MUELLER. The last two I would say are Al-Shabaab in Somalia and what is a substantial concern is a radicalization over the Internet of persons, lone wolves, in the United States. That is the full view of that threat picture.

Mr. SMITH. Thank you, Director Mueller.

The gentleman from Michigan, the most recent Chairman emeritus of the Committee, is recognized for his questions.

Mr. CONYERS. Thank you very much, Chairman Smith.

In our area in Detroit, we are very concerned about improving the relationship of the Muslims, the Arab community with law enforcement. And we are still reeling over that October 2009 shooting where an FBI agent killed a person with 21 bullets. There was an undercover informant involved. And there is a continuing swell, undercurrent of criticism about some of the undercover informants of

the FBI stirring up trouble in the Arab American community, almost as provocateurs. That is a very disturbing situation that I hope is not going on in other communities across the country.

Your comments?

Mr. MUELLER. Well, let me start by saying since September 11th, every one of our field offices, 56 field offices, has had extensive outreach to the Muslim American, Arab American, Sikh American communities with direction from headquarters to do everything you can to develop relationships for individuals and entities associated with those communities. And across the country, I think those relationships are very, very good.

I am familiar with the incident to which you refer in Detroit. I think everyone who has looked at that incident believed that the response was appropriate under the circumstances.

And lastly, with regard to the use of undercover operations, we have used these for probably the 100 years of our existence in terms of undercover operations when it comes to public corruption, on narcotics trafficking, traffic in child pornography. And so the use of undercover operations we do across the board day in and day out. Undercover operations in terrorist cases are not much different than undercover operations that we do across the board.

Secondly, I would say and point out that they are subject to substantial review at headquarters and are monitored as they go forward not only by headquarters but also monitored by the U.S. Attorney's offices in which the undercover operations are taking place to assure that we are not entrapping individuals but there is a predisposition of those individuals to undertake that criminal activity.

And finally, I would say if you look at the number of terrorist threats that were thwarted where individuals were arrested and those individuals would assert the entrapment defense, I am not familiar with a jury that has found in favor of a defendant on the entrapment defense in the many cases that have gone to trial since September 11th.

Mr. CONYERS. We have a recession, a depression in many places, and it stemmed from the subprime mortgage scandal, the bundling up of derivatives and sending them into financial markets all over the world. Wall Street has been thoroughly embarrassed by some of the activity that has been determined. We are passing all kinds of laws trying to put sunlight on some of these activities that are going on.

Not one person has been imprisoned yet. Nobody has gone to jail. Nobody has been punished. The Department of Justice can't come up with any kind of strategy to really use the criminal justice system as it is used for everything else. Could that be because the FBI hasn't done enough work in getting a case built up, the evidence brought in that would result in indictments?

Mr. MUELLER. I strongly disagree with that portrayal of our efforts, Congressman. There have been any number of indictments. We have had takedowns just about every 6 months of persons arrested for mortgage fraud, securities fraud, corporate fraud. There are ongoing trials today in that arena. If you look at mortgage fraud alone, we have over 3,000 cases that we have been investigating. We have got 94 task forces. I have got 340 agents that are directed just to mortgage fraud.

Mr. CONYERS. Yes, but it is not Wall Street.

Mr. MUELLER. With regard to corporate fraud, we have 667 cases, over 55 related to the subprime mortgage industry. Most of these cases are of Wall Street. We have 110 agents that are looking at corporate fraud. When it comes to securities fraud, we got 1,700 cases. I have got 233 agents that are working on securities fraud, and out of those particular initiatives, there have been any number of indictments and convictions. And I would be happy to give you a listing of those indictments and convictions.

And one last point. If you look at the newspapers today and yesterday and the day before, you will see that there are cases that are taking place in New York as we speak with regard to corruption in Wall Street.

Mr. CONYERS. I feel a little better now. [Laughter.]

And I will start reading the papers more carefully.

Mr. SMITH. Thank you, Mr. Conyers.

Considering the gentleman from Wisconsin's role in developing the PATRIOT Act, he is recognized for a very full 5 minutes.

Mr. SENSENBRENNER. Well, thank you very much, Mr. Chairman.

First of all, Director Mueller, let me say that I am going to truly regret your term expiring in September. I was the Chairman of the Committee at the time 9/11 took place. The cooperation between you personally and me personally, as well as the FBI and the Committee, helped us develop I think some very useful legislation, and it was not just the PATRIOT Act, but it was other laws as well that has made Americans safer.

I think on September 12th, 2001, if anybody would have predicted that we would have avoided a major terrorist attack for over 9 years, they would have been accused of smoking something that they shouldn't be smoking. That is a result of the FBI utilizing the tools that the Congress gave them and you directing the agents of the FBI in a manner where there have not been any proven civil rights violations as a result of the expanded provisions given to law enforcement as a result of the PATRIOT Act.

And I would agree with the Chairman of the Committee that there has been an awful lot of hype about the PATRIOT Act that is not actually founded in the 16, subsequently expanded to 17, expanded tools that were given to law enforcement by that act.

Now, all of that being said, we are in the process of fighting over reauthorization. I want to ask you to make some comments about the bill that is pending in the other body since we can't ask the authors of that. So you have got the field to yourself.

The Senate version of the extension sunsets the national security letter standard established under the act at the end of 2013. Do you support reverting back to the pre-9/11 standard for national security letters? And if not, why not?

Mr. MUELLER. I do not. Let me say that the reauthorization that is up does not address national security letters. In other words, the three provisions that are being up for reauthorization do not relate to national security letters. But the national security letters are the building blocks of any case which enable us to collect information, and based on that information, we then can make a further showing to the FISA Court for more intrusive investigative activity such as monitoring conversations or doing searches. Changing the stand-

ard or sunsetting national security letters would adversely impact us if it were sunsetted undercutting our ability to undertake the kinds of investigations that have led to the disruptions in the last 9 years.

Also, having a sunset provision contributes a degree of uncertainty in the months going up to when that provision is to be reauthorized that is unsettling and disturbing in the sense that you don't know where your investigations will be at a particular time when it comes up for Congress' reauthorization. And consequently, quite obviously we prefer not to have that uncertainty, not to have that question about what will be our powers down the road.

Mr. SENSENBRENNER. Now, on another issue, I am fully aware that there are only three provisions of the PATRIOT Act that were sunsetted. I did the hearings 5 years ago, 6 years ago where the other 14—there was really no controversy, and they were made permanent. But there are those that wish to beat the drum and open them up again. And one of those is the delayed notification search warrants where the Senate bill proposes to shorten the time from 30 days to 7 days.

A couple of questions. Has the 30-day notification delay been held unconstitutional or improper? What operational advantages result from shortening the 30 days to the 7 days? And will investigators have an easier time investigating terrorist threats or a more difficult time?

Mr. MUELLER. I think the 30-day time frame works well. It gives you an opportunity to develop the investigation without having to, every week, go back to the court with an additional filing. Every one of these filings are fairly substantial. Every one of these filings—you have to put manpower into it, whether it is from the investigative point of view or from the prosecutorial point of view. I see no advantage to drawing it back to 7 days. It means additional work.

The other thing I would say is that the 30-day time limit is set by the court. So the court is reviewing this periodically, and if the court believes that there is some problem with the 30-day period, the court can go ahead and require a further report shorter if that particular judge who is monitoring this feels that 30 days is inadequate.

So I would be against the change from 30 days——

Mr. SENSENBRENNER. The final question is, does shortening the delayed notice warrant do anything to assist the target of the investigation to evade surveillance?

Mr. MUELLER. I would have to think about that and get back to you on that particular question.

Mr. SENSENBRENNER. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Sensenbrenner.

The gentlewoman from California, Ms. Waters, is recognized for her questions.

Ms. WATERS. Thank you very much, Mr. Chairman.

I would like to say to our FBI Director, Mr. Mueller, I thank you for your 10 years or more of service, and I appreciate the way that you have always been responsive to the Members when we have sought you out for information or clarification. And we are going to miss you.

But before you go, I have to tell you that some of us have been focused on the financial crisis, and just as Mr. Conyers started to talk about what role the FBI have played in bringing to justice some of those who have committed mortgage fraud, for example—it seems that we know some things and we have learned through WikiLeaks and those who received some of the WikiLeaks information about Bank of America and Bank of America is involved with the Balboa organization, insurance organization, and one of their ex-employees who have exposed some information about fraud.

Without going into that specific case, I appreciate the fact that you have indicated that you have all of these investigations going on and you have these agents and the special task force. But this has been going on since 2004. Nobody has gone to jail. Nobody has been identified as a major player in all of this. Meanwhile, people are losing their homes and we find that the servicers who are supposed to do the loan modifications uncover fraud but they do nothing about it because they are not charged with doing anything about it.

What is the FBI doing? Who have you sent to jail? When are we going to get some justice in this area?

Mr. MUELLER. Excuse me just 1 second.

I wish I had brought today the statistics of the persons we have arrested, indicted, and successfully convicted and sent to jail. There are hundreds. And I would be happy, as I told Congressman Conyers, to get those statistics to you.

What I have relayed in response to the question from Congressman Conyers is the efforts that we have made in the last 2 or 3, 4 years to address exactly what you are saying is the problem. And we have been very successful in those efforts. We have had a comprehensive approach, coordinated with the Department of Justice, and through task forces around the country, as well as in New York in the financial arena in New York to address exactly what you pointed out in terms of those factors that contribute to where we are in terms of the economy.

Ms. WATERS. Mr. Director, let me just ask you this. Most of the mortgages are being initiated through the Big Five. You have got Bank of America. You have got Wells Fargo, Chase Manhattan. And they are servicers. They own these servicing operations. This is where the problems are. We don't hear anything about what is being done about fraud from the big servicers who are so-called managing these loan modifications that ignore the fraud, who maybe even participate in it. What has been done on the big operations?

Mr. MUELLER. Let me say that I am familiar with the allegations relating to services. We do have fraud or illegal activity with regard to the services and servicing of mortgages, and we do have open investigations there. I could not in open session discuss with you more specific parameters of our investigations other than to say that to the extent that we have allegations with regard to fraud, we do investigate and are investigating.

Ms. WATERS. Let me just say it starts with the loan initiators, some of whom we discovered, for example, with Countrywide in California who put these loan initiators out on the street without a lot of training and not a lot of background checks. They actually

committed fraud in some cases where they signed the name of the homeowner to mortgages that they did not understand or know about. It starts there, and then from the loan initiators, it goes on to—you know, we have to say that some of those responsible for the secondary market have some responsibility in that. By the time it gets to the servicer, the servicers again are committing crimes. So we have homeowners who have been exposed at three levels by an industry that simply ripped us off. What is going to be done about it?

Mr. MUELLER. They just handed me some of the statistics we have. Back in 2010, we had 217 indictments and informations in the corporate fraud arena, and as of this year, we have had 89.

As an example of a case, in February, last month, Michael McGrath, the former president of U.S. Mortgage, a privately held mortgage company, was sentenced to a jail term of 168 months for his role in orchestrating a $136 million corporate fraud scheme related to the subprime mortgage industry.

Ms. WATERS. What happened with Ameriquest? Did you do anything with Ameriquest, the big one?

Mr. SMITH. The gentlewoman's time has expired, and the gentleman from Florida, Mr. Ross, is recognized for his questions.

Ms. WATERS. Thank you very much.

Mr. ROSS. Thank you, Mr. Chairman.

Mr. Mueller, again, I want to echo the sentiments of the Members of this Committee and congratulate you on your service. It is very distinguished and it has been at a time when this country has needed your type of leadership. So I thank you.

Specifically with regard to the PATRIOT Act and the roving wiretaps, this is something that I find absolutely useful if we are going to continue the type of surveillance necessary to prevent any further attacks. And I guess my question to you is in these roving wiretaps, if it is not reauthorized, what is your recourse in terms of delays.

Mr. MUELLER. Our only recourse in that event is to keep going back to the court as we receive new information that the person has thrown away the first cell phone that they had on day 1 and bought another one for day 2, and we can anticipate another one for day 3.

Mr. ROSS. And how long would that take?

Mr. MUELLER. It takes a good long time, and there is a delay in terms of getting the re-upped order. And so you may well miss conversations as you attempt to draft the application with the affidavit and the proposed order, get it to a court so it can be reviewed and issued. So the consequence is the delay that it takes to get the order and what you may lose in the time frame that it takes you to get that order where you do not have coverage on that particular phone or phones.

Mr. ROSS. And it makes us significantly more vulnerable.

Mr. MUELLER. It can. It can, yes, sir.

Mr. ROSS. With regard to the national security letters, when those have been issued, how have they been received by some of the communications providers? Have you seen any resistance?

Mr. MUELLER. There have been pockets of concern where we have had to use the 215 business records to back up national security letters.

Mr. ROSS. So in other words, they wouldn't give you the substance of the communication. They would just give you the fact that a communication——

Mr. MUELLER. They may give us some information, but not the information to which we believe we are entitled under national security letters which requires us then to go to 215 proviso to obtain the records.

Mr. ROSS. And that too is a delay then.

Mr. MUELLER. That is a delay.

Mr. ROSS. Is there anything we can do to help you there?

Mr. MUELLER. It is a delay.

Mr. ROSS. With regard to the Espionage Act, do you think it should apply to foreign defendants outside of the territorial jurisdiction of the United States?

Mr. MUELLER. I think I know to what you are alluding in terms of ongoing investigations. I unfortunately would have to stay away from opining on the application of the Espionage Act.

Mr. ROSS. I understand.

With regard to gangs, what efforts are being made to investigate and to curtail the growth and involvement of gangs?

Mr. MUELLER. Well, from the perspective of——

Mr. ROSS. I know you have a task force.

Mr. MUELLER. We have over 100 violent gang crime task forces. We have what we call Safe Trails task forces for Indian Country, and we have 41 prostitution task forces or working groups across the country. We have over 1,300 agents who are working gangs throughout the United States.

Mr. ROSS. How is it going? Have you seen an increase, gang activity increase, stabilize, or decline?

Mr. MUELLER. I would have to say that gang activity is increasing not perhaps at the rate it did maybe 4 or 5 years ago, but still, nonetheless, is increasing. I do believe that our work on these gang task forces principally with State and local law enforcement have made a dent in many communities. Our admonition to the task forces to identify a particular sector of the city which has levels of violent crime, address that violent crime and at the end of it, I want to see what impact there has been in reducing the violent crime in that area of the community. And as we focus on that, we do it with our State and local counterparts, and I think we have been effective in utilizing that task force concept in addressing gangs.

Mr. ROSS. And you found good cooperation with the State and local law enforcement?

Mr. MUELLER. Yes, although I continue to urge—when Congress appropriates funds for State and local law enforcement or even for us, there are areas in which there is a great incentive to—as you give an incentive to a State and local law enforcement to cooperate with the Federal authorities, it enhances that cooperation. And consequently our success in the Bureau is dependent on our relationships with State and local law enforcement. And to the extent that Congress in its activity can encourage that, I am supportive.

Mr. ROSS. One last question. What advice would you publicly give to your successor?

Mr. MUELLER. I would say that the Bureau is its people, its agents, its analysts, and its staff. You will never find a greater group of dedicated professionals across the country. Rely on them. They do the job day in and day out, tremendously dedicated. And to the extent that we are successful, it is these individuals. But as I said before, it is also so important to understand that our success is dependent on working with our State and local law enforcement, as well as our counterparts overseas.

Mr. ROSS. Thank you and I yield back.

Mr. SMITH. Thank you, Mr. Ross.

The gentleman from Virginia, Mr. Scott, is recognized for his questions.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Mueller, it is good to see you today.

Talking about Medicare fraud, there have been reports that billions of dollars are being siphoned off by criminal activity. 60 Minutes and other exposes have shown it is widespread and easily done. When you have FBI agents chasing after Medicare fraud, do they produce more in savings than they cost?

Mr. MUELLER. I would have to get back to you but I absolutely believe that is the case.

Mr. SCOTT. Say again?

Mr. MUELLER. Absolutely, I believe that to be the case. I would have to give a close look at it, but I do believe that is the case.

Mr. SCOTT. And in the mortgage fraud, you have been back and forth on that. The fraud was so widespread. Are you seeking civil fines from a lot of people that got illegal profits?

Mr. MUELLER. I know the Department of Justice—and we are helping the Department of Justice in certain instances in seeking civil fines, but we also, whenever we can, would seek outright forfeiture of any ill-gotten gains. And we have been successful in doing that.

Mr. SCOTT. You have agencies where just the whole company profited through corrupt practices. Is there any widespread effort to get—I mean, if you go through, there are billions, trillions of dollars of illegal profits that ended up with the total collapse of our economy. Is there any effort to recover those illegal profits——

Mr. MUELLER. Yes.

Mr. SCOTT [continuing]. On a widespread basis?

Mr. MUELLER. Absolutely. Initially we will look at it for criminal forfeiture to the extent we can identify the ill-gotten gains and tie it into the fraudulent scheme. Secondly, we would go after it, and by we I mean the Department of Justice civilly. And thirdly, you have private actors that we would go after and seek the ill-gotten gains. Perhaps the Madoff case is the most notorious example of that kind of attempt to recoup the losses to——

Mr. SCOTT. And you are doing that on other cases too?

Mr. MUELLER. Pardon?

Mr. SCOTT. You are doing that on other cases too?

Mr. MUELLER. Absolutely.

Mr. SCOTT. There are two areas, organized retail theft and ID theft, where a lot of crimes could be solved if you had the man-

power to actually do the legwork because there is usually a paper trail. Do you have enough agents working on organized retail theft and ID theft to be an effective deterrent?

Mr. MUELLER. Let me just talk about organized retail theft. We will, in particular areas of the country where there is a need for us to assist State and local law enforcement in addressing it or there is some sort of organized criminal activity that cuts across jurisdictional lines, allocate the personnel to address it, generally in the task force paradigm.

ID theft. Again, we will work with our State and local counterparts. There are a number of task forces and working groups to address ID theft, but I will tell you that it is so prevalent. It is very difficult to comprehensively address that, and our resources are relatively thin, particularly when it comes to——

Mr. SCOTT. But if you had more resources, you could do more work on ID theft.

Mr. MUELLER. More resources, we could do more in terms of ID theft and a number of other areas.

Mr. SCOTT. Are there any loopholes in gun laws that need to be closed?

Mr. MUELLER. That is a very broad subject. I would have to look at a particular piece of legislation to opine on where we should be in that area.

Mr. SCOTT. Well, if you could get back to us with recommendations, that would be helpful.

Mr. MUELLER. Thank you, sir.

Mr. SCOTT. My time is running out. If you could comment generally for the record on any problems that the FBI lab has, any challenges they have. If you could just get back to me on if there are any challenges, things we need to look at.

There is a disconnect around here about cutting a budget and what will not get done. If you could provide examples of what would not get done if some of these proposed budget cuts are passed, that would be helpful.

Finally, you indicated on the criminal side as opposed to national security you needed the lone wolf provision, and the lone wolf provision requires a determination of terrorism. How do you get those without the same information that would allow you to get a title III warrant? Or why do you need the PATRIOT Act provisions rather than—because if you have evidence that he is a terrorist, that should be enough evidence to get a title III warrant, and the same with some of the other provisions.

Mr. MUELLER. That is not necessarily true. On the title III and the criminal side, you are looking for a person who has committed or is in the process of committing a crime. On the national security side, you are trying to prevent that terrorist act and identify that person as a terrorist. The glitch is that you have to show without this statute that the person is an agent of a foreign power in order to get that warrant on the FISA side, which if it is a terrorist group, as we saw in the Moussaoui case, may be difficult to do.

There is another aspect to it and that is often on the counter-terrorism side and since September 11th, we integrate information from the CIA, NSA, and other intelligence entities. There are provisions on the national security side to protect that information, the

sources and the methods that you do not have on the criminal side. And consequently, the mechanisms we have on the FISA Court and the FISA statute allow us to do often that which cannot be done on the criminal side and where the focus is an agent of a foreign power, the agent of a foreign power in this case being a terrorist.

Mr. SMITH. Thank you, Mr. Scott.

The gentleman from South Carolina, Mr. Gowdy, is recognized.

Mr. GOWDY. Thank you, Mr. Chairman.

Director, I want to commend you for your service not just with the Bureau but also as a Federal prosecutor. I had the privilege of meeting you in South Carolina many years ago when you came down to our State Law Enforcement Division, also known as SLED, for a computer. And I also want to take this opportunity to compliment your agents in the upstate of South Carolina, specifically Spartanburg and Greenville. They worked, along with the DEA, a public corruption case which saw a magistrate judge and an elected clerk of court go to prison for selling evidence, selling drugs out of the evidence locker. And to the extent you are going to be in South Carolina before your term expires, if you would tell Special Agents Mike Kelly, Brian Bryan, and Jim Lannamann how grateful all of us are for their hard and excellent work. They really are a credit to the Bureau.

Mr. MUELLER. I will pass that on, sir. Thank you.

Mr. GOWDY. They have been wonderful. I got to work with them for 16 years as a prosecutor and there are days I miss that job. [Laughter.]

Mr. MUELLER. So do I. [Laughter.]

Mr. GOWDY. Maybe we can go back together and be on the side of the angels and prosecute again.

I wanted to ask you about mortgage fraud and health care fraud. You have already addressed those. I would ask you specifically with respect to health care fraud, I don't know whether this statistic is correct or not. I suspect it probably is: 48 different agencies or sub-entities that have jurisdiction with respect to investigating health care fraud. Is there a more streamlined approach and therefore more effective approach that you could recommend? Does the Bureau ever bump into other agencies when you are investigating health care fraud? Is there a better way than the way we are doing it?

Mr. MUELLER. Having been a prosecutor, you know we do bump into other agencies, and when we bump into other agencies, we try to incorporate them in a task force. If you look in Florida and Texas and around the country, the major successes have been undertaken in utilizing the task force concept where many of those 60-odd agencies that you mentioned are participants. And it is not just the Federal. It is not just HHS and the IG or the FBI or the Postal Service. It also is State and local attorney general offices, local district attorney offices that participate in these task forces, and you find you are able to triage the cases. The more substantial ones will go to Federal court. The ones that can be addressed in State court are then triaged and addressed in State court. What you try to do is identify the universe of cases and then make certain that every one of them is addressed in one way or another. Again, the task force concept is the way to go, and we have any

number of task forces and working groups around the country addressing health care fraud.

Mr. GOWDY. Using both your law enforcement hat and your prosecutorial hat, are there any categories of declinations that the Bureau is receiving from U.S. Attorney's offices that you find troubling? Are you working a certain category of cases and just not having them indicted or prosecuted? And I am not trying to put you on the spot with U.S. Attorneys. But are there any categories of cases that your folks could use some help with in terms of maybe a disproportionate number of declinations?

Mr. MUELLER. No. I don't think the issue is declinations, but having been a U.S. Attorney and now an investigator, the one thing I do say is that we have to together address white-collar criminal cases swiftly, effectively, and move on to the next. One can get bogged down in the paperwork and the intricacies and the desire for a number of counts and where we have a large backlog of cases, as we do, for instance, in the mortgage fraud area, we have to go through and push those through both from the investigative side as well as from the prosecutor's side. And I have found that prosecutors around the country understand that and are giving us the support that we need to continue to investigate and prosecute these cases.

Mr. GOWDY. My time is almost up, so I will ask you one more question and then finish with one quick comment.

Any changes that you would like to see in the sentencing guidelines?

Mr. MUELLER. Not offhand. I would have to get back to you on that. I really have not given that much thought recently.

Mr. GOWDY. Well, I will close by the same way I started, thanking you for your service in law enforcement and also as a prosecutor.

Mr. MUELLER. I will see you back in the courtroom. [Laughter.]

Mr. SMITH. Thank you, Mr. Gowdy.

The gentlewoman from Texas, Ms. Jackson Lee, is recognized for her questions.

Ms. JACKSON LEE. Director Mueller, thank you, first of all, for your service. We have had the mutual privilege, I would claim, at this point to see each other on a number of occasions over the years, and I know that we have gone through some enormously tough times.

I want to focus on what I think is a rising but certainly a crisis that our combined law enforcement have really tried to counter and that is the drug violence on the Texas border or on the southern border. I would like to get your assessment. We know that President Calderon is coming to the end of his term. We know that there have been 35,000 deaths plus. We know that two teenagers left El Paso and didn't make it back from the other side of the border. We know that the mayor of Laredo has been here pleading for a focus.

My question is obviously we have the Border Patrol, but the FBI, as I understand it, are in a number of drug task forces, gun-running task forces. I would like to know what progress we have made. What can we claim as victories with the task force structure

that we have used to try and get our hands around this question? That is number one.

What is the level of gun-running that you have assessed specifically out of Houston, Texas or coming from the United States into Mexico?

Number three, I do believe you could be a vital advocate. Some of us said that we tire of seeing fallen law enforcement officers, just recently a U.S. marshal, certainly Mr. Zapata in Mexico, though he was, as we understand it, under those laws unarmed, but fallen law enforcement officers in the line of duty. We honor them every May 15.

Speak specifically to the question of clips being sold randomly over the counter, if you will, ammunition clips, and speak specifically to a background check for private sellers and how that would be helpful and not harmful. What harm could that do?

And I might say, Mr. Mueller, that what is not left to the Federal Government certainly is the States, but in this instance I consider the lack of reasoning gun regulatory process and unfunded mandate to the States and the cities dealing with the fallen, whether it is our law enforcement officers or the bloody Friday and Saturday nights that come about through local gang warfare, methamphetamine fights, cocaine fights, whatever fights you are having. That is an unfunded mandate that this Federal Government is not answering.

So if you would for a moment give us the real impact of $133 million in cuts or more as we make our way through this budgeting process. Mr. Mueller?

Mr. MUELLER. Let me go back and start on the first question I think related to Mexico and what we see on the border and what successes there might be down there. I do believe President Calderon has undertaken an unprecedented attack on the cartels and violence in Mexico. Unfortunately, it has not been as successful as he or anybody else would like, given the murder rate and the atrocities that occur south of the border.

I do believe one of the—and I am not certain I would call it a success. I would say at this point in time we have not seen wholesale violence north of the border. We have the incidents of law enforcement shootings, the ICE agents in Mexico and then customs enforcement agents in the United States. We have had in several of our cities over the past several years kidnappings where individuals who have businesses or family in Mexico but they are living in the United States will be kidnapped. We put together task forces to address that, and I do believe that those incidents have been reduced as a result of that.

We also in the FBI particularly focus on corruption at the border. We have got a number of task forces that address corruption. They have been successful in rooting out corruption north of the border.

And lastly I would say we contribute with our border offices as well as our legal attache office in Mexico to a unified intelligence task force operating out of El Paso that is, I believe, a substantial advance in providing intelligence, not just individuals, our counterparts in Mexico, but also to those who are operating along the border to prevent that violence from coming north of the border.

We recently addressed one of our concerns which is the gang, Barrio Azteca, which has grown over a number of years both in Mexico as well as in the United States. We had a takedown and arrest of a number of the principal players in Barrio Azteca several weeks ago. That also was an important step.

You asked about the extent of guns going from Houston, if I am not mistaken, down south.

Ms. JACKSON LEE. And if you could include in that the clips. Just answer specifically clips legislation and background checks.

Mr. MUELLER. Neither on the guns nor the clips do I really have an understanding of the extent of the gun-running from north of the border to south of the border. I would have to get back to you on that.

As to the gun laws and modifications to the gun laws, I don't think there is a person in law enforcement who isn't tremendously disturbed when any law enforcement agent in whatever entity loses his or her life. And there have been a spate of those killings recently, unfortunately, and the number of law enforcement that died in the course of duty last year was up from the year before. And without getting into specifics, there is not a one of us who wouldn't like to see some sort of capability to address automatic, semi-automatic and large clip weapons. When it gets to the specifics, I will leave that up to others, but all of us in law enforcement are concerned whenever any particular law enforcement agent goes down. Unfortunately, it is not getting better, it is getting worse.

Mr. SMITH. The gentlewoman's time has expired.

Ms. JACKSON LEE. Mr. Chairman, can I just ask a question to you, please?

Mr. SMITH. Of course.

Ms. JACKSON LEE. And Mr. Mueller could hear the question.

Two questions. One, I think it would be appropriate for a classified briefing on the drug violence and drug task force in particular. Some of the information is classified and I would just encourage the Ranking Member and the Chairman to consider such a briefing.

And then to Mr. Mueller, I would like to engage with the task force in Houston and would ask the FBI to cooperate. I will be seeking to engage with a meeting and just getting the sort of overall briefing as to what is occurring.

Mr. Chairman, I just want you to know there is gun-running in Houston, and it is challenging. But I appreciate the fact that if we could have a briefing, you could consider that.

Mr. SMITH. We will certainly consider that. Thank you for the suggestion.

The gentlewoman from Florida, Ms. Adams, is recognized for her questions.

Ms. ADAMS. Thank you. Thank you for your service. As someone who has worked in an undercover capacity on a task force with the FBI in a previous life as a deputy sheriff, I understand the intricacies involved when you are doing investigations. And while a lot of people want it to hurry up and get to the fruition, sometimes it is not that easy. And if you do want a conviction, you want to make sure that you have every "I" dotted, every "T" crossed, and ensure that when you bring that information to the courts, that the courts

will be able to go forward with that conviction. So I want to thank you for your service.

I want to get back to the roving wiretaps because I have heard a lot about it in Committee meetings and everything, and I have heard some people say that you don't have your target identified. Now, as someone who has been involved in these type of investigations, I know that you have to have a target identified before you can get this type of tap. Correct?

Mr. MUELLER. Correct.

Ms. ADAMS. It may not be you have the accurate name. They may have 20 names associated with the same person, but you have your target identified.

Mr. MUELLER. Exactly. You have it exactly right. We have to go to the judge with sufficient information to identify this individual from all other individuals. We may not have an accurate name, as you indicate, on the individual, but nonetheless, we may have been surveiling him for a period of time. We may have information on somebody. The name is affixed to this particular person, but we don't know the true name. But we, in order to get the warrant, have to have sufficient specificity to identify this individual from all others.

Ms. ADAMS. I have been in those situations when I have been trying to obtain a warrant myself.

Let me get back to the PATRIOT Act, and I want to ask you what unique challenges to investigations and to terrorism prevention efforts are posed by the self-radicalized jihadist?

Mr. MUELLER. Having been in law enforcement yourself, one knows that it is somewhat easier to make a case when there are a number of individuals who are conspiring together. One will crack. You will get communications. There will be some telltales that will enable you to pursue the investigation. If you have a person who is self-radicalized, for instance, on the Internet, and his association is with the Internet and with other persons who are anonymous on the Internet, and that person watches videos and that person continuously educates him or herself in terms of getting to the point where they are willing to undertake terrorist attacks, they are very, very difficult to discover because there is no outreach to others. There is no communication. You can't identify a person lower in the chain or up the ladder that will identify him. And so it is a real challenge for us in law enforcement to be able to identify those persons before they undertake a terrorist attack.

Ms. ADAMS. I listened to the last questioning and I heard your answers. I too am concerned about what appears to be targeting of our law enforcement personnel across our Nation and those working outside, as what happened in Mexico. I have a husband who is on the wall at Judiciary Square, along with a lot of my friends. So I have a true understanding of this issue.

I am concerned, however, that we send men and women across the border and they aren't armed. So I know that wasn't your agency, but it does concern me enough that I want that on the record that we need to do more to give our men and women the tools they need when we are TDYing them or sending them into such an area.

Now, the lone wolf provision and how it works. We have heard so much here about the PATRIOT Act and that it is going to target American personnel. And that is not what it does. Is that correct?

Mr. MUELLER. This is for a non-U.S. citizen. That specific provision is applicable only to a non-U.S. citizen. And that is perhaps unique to that particular provision, but it is in that provision. The fact that it applies only to a non-U.S. citizen is in that particular provision of the statute.

Ms. ADAMS. Thank you.

Well, again, thank you for your service. I want to thank your men and women. I have worked with them before on task forces. They are very professional and I appreciate all that you do.

Mr. MUELLER. Thank you, ma'am.

Mr. SMITH. Thank you, Ms. Adams.

The gentleman from North Carolina, Mr. Watt, is recognized.

Mr. WATT. Thank you, Mr. Chairman.

Director Mueller—I always have trouble with the name, but I think I got it right this time.

When you have been before the Committee before, I have asked you about a whole range of different issues. But I am going to put on my Ranking Member hat of the Intellectual Property Subcommittee this time and try to focus attention on some issues there.

We recently, in fact yesterday, had hearings on proliferation of counterfeit goods in both the domestic and international marketplace and examined the issue of piracy of copyrighted items such as movies and luxury items on rogue sites based in foreign countries. One of the things that we found was that clearly reacting to this is going to require a coordinated response between multiple law enforcement agencies, the FBI, Department of Justice, Homeland Security, ICE, and the Patent and Trademark Office, if we are going to effectively be able to address the problem.

I am interested in your assessment of the extent to which those different agencies are coordinating their efforts, whether you feel like you have crafted a coordinated effort in this area, and if so, discuss how this has worked in practice and whether jurisdictional and oversight challenges that we have here in Congress even between the agencies have arisen.

It has never really even been clear to me whether ICE is under Homeland Security, whether it is under the Department of Justice, whether it is under the FBI. I don't know where it is. Maybe you can clarify that for me in the process of responding to that question.

Mr. MUELLER. Yes, sir. Let me start off by saying that ICE is in the Department of Homeland Security.

Going to the issue of how we address intellectual property, we obtained, I think, an additional 20 slots for agents specifically to focus on intellectual property last year, 2010. I believe we are still in the process of allocating those resources, but allocating those resources so they would maximize the impact. Not doing one in an office here, one in an office there, but looking at where we can most effectively align those agents to have the maximum impact on what is a huge, huge problem.

I will tell you that our focus to date has been on intellectual property as it relates to health and safety. An example is an investigation we had some time ago into counterfeit aircraft parts where it goes beyond just the loss of money but could adversely impact the life of persons.

And so when it comes to intellectual property, we do have additional resources. We are trying to allocate those additional resources to address the problems, and I would say we would do it again in the context of task forces with ICE agents, with agents who also have jurisdiction so we can together maximize the impact.

Mr. WATT. So you feel like you are coordinating effectively in this area? Because there still seem to be yesterday just a crying out of almost a helpless feeling on the part of the people in industry about the extent of piracy and rogue sites that are selling pirated goods or whatever.

Mr. MUELLER. I would have to get back to you on the extent and whether there are any issues with regard to that coordination.

Mr. WATT. Get back to me on that and also on the question of whether you feel like—you said you got 20 additional personnel, but specifically whether you are adequately resourced to investigate and prosecute these cases because, as I said at the hearing yesterday, the extent of the problem far, far exceeds bank robberies in the old-fashioned way. In fact, most bank robberies now are taking place through technological advances also. Nobody is walking into a bank with a gun anymore.

Mr. MUELLER. We still have those.

Mr. WATT. Yes, I know you do, but everything I have heard suggests that a lot more money is being stolen from banks electronically——

Mr. MUELLER. I would agree with that.

Mr. WATT [continuing]. Than in the old-fashioned with a gun way.

I think I may be out of time. I had one other question, but I don't want to abuse the privilege and I will yield back.

Mr. SENSENBRENNER [presiding]. The gentleman from Texas, Mr. Poe.

Mr. POE. Thank you, Mr. Chairman.

Director, good to see you. In my other life, I was a judge in Houston and I used to tell the FBI to bring me some business, but we don't do that anymore. So it is good that you are here and appreciate your work.

I want to talk about Brian Terry. Are you all taking the lead role in the investigation of his murder? The border agent.

Mr. MUELLER. Oh, yes, we are absolutely.

Mr. POE. I understand the investigation is going on, but I have heard through media reports that Brian Terry was armed at first with a bean bag gun and had to fire that first before he could use—to fire back at those drug cartel members that were using AK-47's. I don't know if you can comment on that or not. If you cannot, I understand. But can you say anything about that?

Mr. MUELLER. I cannot say anything about that, but I do know that Janet Napolitano has addressed that particular issue in her testimony before another panel.

Mr. POE. Do you see a trend of those drug cartel members that come in the United States becoming more aggressive and violent?

Mr. MUELLER. Well, I think over the last year, certainly we have seen extremes in violence south of the border. I do not believe that those extremes in violence have crossed the border into the United States so far, but we have to be wary of that and work together and by ourselves with ICE, Customs, and Border Patrol and others who are responsible for law enforcement on the border.

Mr. POE. Let me address a specific concern on the Texas border. 16 border counties in Texas consider themselves border counties, and they have a tremendous problem with cross-border crime. I don't want to use the term "violent crime." I just want to use the term "crime." And periodically I will call the sheriffs of those 16 counties and say how many people are in your jail who belong to some other country. It doesn't make any difference to me whether they are here legally or illegally. And at any given time, on an inexact percentage, it is anywhere from 37 to about 45 percent of the people in their jailhouse belong to some other country. They are in the U.S. They are not charged with immigration violations. They are charged with cross-border crime.

I personally think that that is a tremendous amount of folks that are housed in our local jails from foreign countries that are committing crimes in the United States. Can you address that? I mean, do you see that as a problem?21Mr. MUELLER. Well, that gets into an issue that is somewhat removed from the FBI in terms of immigration and the like. And so I prefer to just stay away from that.

Mr. POE. Well, it is not an immigration issue. It is a crime issue. People that cross the border from foreign countries—it doesn't make any difference whether they are here legally or illegally, and a lot of them are in our border jails charged with crimes. Now, I know State and local crimes aren't an issue of the Federal Government and the FBI, but I take a little issue with the fact that there is not crime on the border because the sheriffs are overwhelmed with cross-border crime. And I would think that the FBI should be concerned about that and should help out when they are needed to help out.

Mr. MUELLER. I can tell you that we do help out. We understand, particularly when it comes to violent crime. In particular, to the extent that we can assist State and local law enforcement, we want to be able to do that and we do.

Mr. POE. The cooperation—candidly tell me what you believe the cooperation with the Mexican law enforcement is in the investigation of homicides of Americans in Mexico. I understand there were 65 Americans killed last year in Mexico. To my knowledge, none of those cases have been solved. What is the level of cooperation by them with the FBI in solving those crimes?

Mr. MUELLER. I think it fair to say that it depends on the particular case and the individuals with whom you may have a relationship across the border. We have border liaison agents and officers that spend a great deal of time developing those relationships with our counterparts south of the border. And in many cases, we have a very good relationship and they will do a very competent job and we will work a case well together. There are other cases that do not work out so well.

Mr. POE. Well, not solving 65 murders doesn't sound like a very good clearance rate to me, and I would hope that you would help us to determine how we can get the Mexican Government more involved in helping you in solving these crimes of Americans that are murdered.

My last question is this. The Los Zetas, one of the most violent of all the criminal gangs—do you have an opinion or give some insight on what you think we could do as Members of Congress? Should we try to make them a member—or put them on the foreign terrorist organization list so we could prosecute them better when they commit the crimes in the U.S.?

Mr. MUELLER. I am not certain that that would assist us. Again, as I indicated before, I believe the answer to many of these threats that we face today is the cooperative efforts of State and local law enforcement working with the Federal law enforcement, not only because of the skills and capabilities that are brought to the table by these various entities, but also by the use of both State laws as well as Federal laws to address the activity. And so I would go back to, as opposed to designating a group as a terrorist group where it may not fit that particular category, one focuses on developing incentives for us to work together, particularly financial incentives to work together on task forces to address these.

Mr. POE. Thank you, Director. I appreciate it, Mr. Mueller.

Mr. SMITH [presiding]. Thank you, Mr. Poe.

The gentleman from Illinois, Mr. Quigley, is recognized.

Mr. QUIGLEY. Thank you, Mr. Chairman.

Good morning, Director. Again, thank you for your service.

I guess I can't get off that issue. Again, talking about the border issues, Secretary of State Clinton said that the vast majority of the guns being used are coming from the United States. I can't help but want to ask you a little bit more about how those purchases are taking place, the straw purchasers and the difficulties there, but just across the country in tracking weapons used because of limitations imposed by the laws.

Mr. MUELLER. Well, I would have to defer to my counterparts in ATF who are much more knowledgeable in terms of the flow of guns to Mexico from the United States. From our perspective, whenever we have a case that may involve guns that have been purchased through straw purchasers or there may be other indicia implicating wrongdoing in the purchase of that particular weapon, we coordinate with ATF. We make use of the ATF databases, and our agents are alert to the fact that this is a substantial issue. We have to prohibit the guns, prevent the guns going south of the border, and we do that in coordination with the ATF.

Mr. QUIGLEY. But you have no problems tracking weapons used in crimes across the country. There is no limitations that you can speak of today?

Mr. MUELLER. In terms of tracking weapons——

Mr. QUIGLEY. From their original purchases.

Mr. MUELLER [continuing]. Again, I cannot think of limitations in terms of our ability to do it, but of course——

Mr. QUIGLEY. Language that was passed before limiting access and serial numbers and use of purchase—through purchasers.

Mr. MUELLER. I am not familiar with the intricacies of that discussion.

Mr. QUIGLEY. At least perhaps gun shows, the fact that there is no background check required in a gun show.

Mr. MUELLER. I know that is a subject of discussion in Congress, yes.

Mr. QUIGLEY. Wouldn't it be a subject of concern for you and your agents?

Mr. MUELLER. To the extent that we can track weapons back to individuals and trace weapons, it is beneficial to us in doing our job.

Mr. QUIGLEY. All right. Well, we will shift gears here.

The Supreme Court struck down the honest services law that helped your agency deal with public corruption. How much of a gap do you see this having left in the laws you need? Do you have any suggestions as to specific aspects? The Court said it needed to be less vague, but specific issues there that you feel should be included in any new legislation?

Mr. MUELLER. I have not looked at this issue in a while. I know there was discussion about additional legislation that may partially fill the gap or be responsive to the concerns of the Supreme Court. We, along with the Department of Justice, have gone back and looked at every case that has been affected by the decision, and for the most part, the individuals were prosecuted on mail fraud or other charges as well and most of the convictions have stood up. So in terms of impact on past cases, I think it has had a relatively marginal impact on past cases. And I would have to get back to you on whether or not we need some additional legislative fix to fill that hole.

Mr. QUIGLEY. Earlier the lone wolf provisions were brought up, the PATRIOT Act. From my perspective, many of the lone wolf issues have been not foreigners but American citizens. You probably heard about the fake bomb put near Wrigley Field just this last year, a block from my house. So it is near and dear to home. Do you feel that you have enough tools to deal with the lone wolves who are just American citizens that pose the same threat?

Mr. MUELLER. I am not certain it is a question of additional resources. We are focused very intently on lone wolves, domestic lone wolves, and have been certainly ever since 1995 and McVeigh who was responsible for the Oklahoma City bombing. And we utilized all of our techniques to try to identify the lone wolves, but it is very, very difficult. I am not certain I could say to you today that we need additional resources that I would put here which would improve our ability to identify the lone wolf. We are going to have to adapt additional capabilities and techniques to identify the mechanisms of radicalization so that we then can identify the persons who are the lone wolves.

Mr. QUIGLEY. Thank you. I yield back.

Mr. SMITH. Thank you, Mr. Quigley.

The gentleman from Iowa, Mr. King, is recognized.

Mr. KING. Thank you.

Director, on your left wing over here.

Mr. MUELLER. Sorry, sir.

Mr. KING. Thank you. I am not in the middle of the action here, but I am connected to what is going on.

I appreciate your service to this country and your testimony here today and your responses to your questions.

I would like to take you to a question that deals with Khalid Ali-M Aldawsari. I see you recognize his name even though I might not have pronounced it right. It is my understanding that he arrived here on a student visa, but he is under a charge of attempted use of a weapons of mass destruction. In his journal he wrote, the need to obtain forged U.S. birth certificates, multiple driver's licenses, and U.S. passports. And it is my understanding he planned to use those driver's licenses to rent several cars and to do so with a different license so he could have a different name on each one in order to confuse law enforcement authorities.

Are the driver's licenses and passports and fraudulent—are they a useful tool for terrorists?

Mr. MUELLER. Well, let me start by saying that there is a gag order in that case that has been issued by the judge in al-Dawsari. So I cannot specifically speak to that case.

But speaking more generally, apart from that case, the use of driver's licenses as what we call a seed document that builds a separate identification, yes, that is a problem, has long been a problem, and one that we are knowledgeable about and in every case look to see whether that has been the case that a person's identification has been developed as a result of a seed document such as a driver's license.

Mr. KING. I remember that language now. I hadn't brought it up in some years, but the seed documents from low standards for issuing driver's licenses or false identification that might result in a passport turns into a useful tool for terrorists in this scenario that is generally speaking that you have spoken to.

Mr. MUELLER. True.

Mr. KING. Thank you, Director.

I would go on to something maybe a little bit easier and that wasn't actually hard. These are just a series of questions, but is it common for local law enforcement to work closely with the FBI? And yes. And I grew up in a law enforcement family and I respect that relationship that is there.

And do local law enforcement routinely conduct investigations that result in indictments under Federal charges?

Mr. MUELLER. Yes.

Mr. KING. And do they have the authority to do so?

Mr. MUELLER. Yes.

Mr. KING. And so I take this to this point which is that includes immigration law.

Mr. MUELLER. I guess I don't understand the question.

Mr. KING. The question would be then local law enforcement routinely works with the FBI. They routinely do investigations that result in indictments under Federal charges. So they do so with Federal law and they do so routinely with Federal immigration law as well. And the follow-up question to that is, is it your position that local law enforcement has the authority to investigate and cooperate in the enforcement of Federal immigration law?

Mr. MUELLER. I think that is an issue we would have to get back to you on. It is a little bit removed from the usual issue that we deal with day in and day out when we are looking at a narcotics trafficker and the like. Again, I am not sufficiently well versed in that aspect of the law. We would have to get back to you.

Mr. KING. I would ask you to do that and then I would ask you also to review a couple of circuit court cases, Tenth Circuit. They both happen to be U.S. v. Santana Garcia and the other one is U.S. v. Vasquez Alvarez that I believe are on point for that. And I think it is useful for us to understand that relationship and the cooperative effort between Federal and local law enforcement.

Another subject matter that I am curious about is that there are estimates out that there are roughly 1,200 mosques in the United States, and we are seeing homegrown terrorists emerge, people that have American citizenship by birth that turn against their country. I believe that there is jihad being preached in some of those mosques. Can you tell me is the FBI restrained from investigations in a public setting like that? Can they go into the mosque, listen, report, record? Are you constrained in any way from that type of activities? It might give us a better sense of how the homegrown terrorists are being radicalized.

Mr. MUELLER. I am not certain about the figures that you use, but I will say that we are not constrained in undertaking investigations, but we are exceptionally sensitive to the fact that the First Amendment does protect speech and association. And so we are not constrained in following a predication of an individual regardless of where they may be; who may be contemplating involvement or engagement in supporting terrorism or a terrorism act.

Mr. KING. Does it require a warrant for an FBI agent to sit in a mosque with a tape recorder in a public setting?

Mr. MUELLER. It depends on the circumstances, but generally I would say no.

Mr. KING. Thank you. That helps me a lot.

Mr. MUELLER. In the same breath, I would say that there has to be predication for utilizing that particular technique.

Mr. KING. And just one brief question, if the Chairman would indulge.

Mr. SMITH. Please be brief.

Mr. KING. Thank you, Mr. Chairman.

And that is, Director, do you know of even a single case where an individual had their rights to privacy usurped under the PATRIOT Act that has any potential of being successfully litigated on constitutional principles?

Mr. MUELLER. I don't believe so. I am not aware of one.

Mr. KING. And I don't either. Thank you, Director. I appreciate it.

Thank you, Mr. Chairman. I yield back.

Mr. SMITH. Thank you, Mr. King.

The gentlewoman from California, Ms. Chu, is recognized for her questions.

Ms. CHU. Director Mueller, I have similar questions but from a different perspective.

I believe that you have stated that protecting America requires the cooperation and the understanding of the public. You have also

emphasized that since 9/11, the FBI has developed an extensive outreach program to Muslims, South Asian, and Sikh communities to develop trust, address concerns, and dispel myths in those communities about the FBI and the U.S. Government. And as part of this effort, in 2009 the FBI established the Specialized Community Outreach Team, composed of special agents, analysts, community outreach specialists, and personnel with language or other specialized skills.

Now, as you know, last week the House Homeland Security Committee held a controversial hearing on the extent of radicalization in the Muslim community focusing only on one community. I am deeply concerned about the attempts to marginalize an entire minority group in this country, and the reason I am sensitive to it is that I know that targeting like this can result in great tragedy. For instance, the words "national security" were used to send 120,000 Japanese Americans to prison camps throughout America during World War II, making them lose everything that they had, and in the end, not a single act of espionage was proven.

So considering the efforts to be concerned about improving national security, I would like to ask you if you agree with Congressman King's assessment that American Muslims are not cooperating with law enforcement, especially since Sheriff Lee Baca stated in that hearing that Muslim Americans helped foil 7 of the 10 plots that were launched by al-Qaeda in the U.S.

Mr. MUELLER. Well, I would prefer not to comment on the representations of others. But if the question is to what extent has the Muslim community cooperated with the FBI since 2001, I can say in a number of cases the Muslim community has either initiated or cooperated with the investigation throughout the course of the investigation leading up to a successful disruption of the terrorist plot, often with consequent arrest and prosecution.

Ms. CHU. And is it true, as Sheriff Lee Baca said, that Muslim Americans helped foil 7 of the 10 plots that were launched by al-Qaeda in the U.S.?

Mr. MUELLER. Again, I am not certain of the statistics. I will say that the Muslim community has helped in a number of cases that we have addressed since September 11th.

Ms. CHU. Well, according to a study by the Triangle Center on Terrorism and Homeland Security, the number of Muslim Americans involved in terrorist acts against the U.S. dropped by more than half in 2010 compared to 2009, which seemed to indicate that perhaps we are going in the opposite direction with regard to Muslim Americans being radicalized, as was alleged in the hearing. 20 Muslim Americans were arrested for terrorism crimes last year, which is down from 47 the previous year, and more non-Muslim Americans were involved in terrorist plots last year than Muslim Americans, according to the study.

I would like to have your comments on the findings of this study.

Mr. MUELLER. I have not had an opportunity to review the study, so it would be difficult for me to comment on it.

Ms. CHU. Well, then could you comment on how you think the relationship between the FBI and the Muslim community might be improved?

Mr. MUELLER. I think we continuously have to work at outreach. The FBI certainly does, and I think we have made substantial efforts and they have been successful since September 11th, but it is an ongoing process. Actions of the FBI could be misinterpreted. We use every opportunity we have to explain what we do and why we have done it. Occasionally it is shrouded in secrecy because either the subject matter or the techniques are classified. But to the extent that we can be transparent and point out why we undertake certain actions, the results of those actions, then we find that whether it is members of the South Asian or Muslim or Sikh or Arab American community, there is understanding and we develop, I would say, a very good relationship. We have, I believe, very good relationships with the Muslim community around the country.

I will say, as I have said before often in testimony, that the vast, vast majority of Muslim Americans are no different than any other American sitting in this room or as patriotic and express that in ways that are appropriate in terms of assisting us in our investigations. And we continue to develop the relationships.

One other thing I do believe is the worse thing that could happen to the Muslim community is to have another terrorist attack, and members of the Muslim community understand that, respond to it, and for the most part, are cooperative.

Ms. CHU. Thank you. I yield back.

Mr. SMITH. Thank you, Ms. Chu.

The gentleman from Arizona, Mr. Quayle, is recognized for his questions.

Mr. QUAYLE. Thank you, Mr. Chairman.

And thank you, Mr. Director, both for your service and for being here today.

Now, we have the PATRIOT Act reauthorization for a certain number of provisions. I just have one question regarding the roving wiretaps.

Now, when an order authorizing the roving or multi-point wiretaps, what type of reporting to the court is required when a new communications facility is actually identified?

Mr. MUELLER. Would you excuse me just a second?

Mr. QUAYLE. Yes.

Mr. MUELLER. Yes. I wasn't familiar with the details, but apparently we make a return within 10 days of the new phone number. So there is a responsibility to get back to the court and alert the court as to the fact that there was a new number.

Mr. QUAYLE. And this is after they have already gone to court to get the initial authorization.

Mr. MUELLER. Yes, sir.

Mr. QUAYLE. Thank you.

And moving on to a different topic, cyber security is going to be a potent threat going forward. It already is now, but going into the future, it is going to be even more dangerous. What is the FBI's role in assessing and investigating various cyber threats?

Mr. MUELLER. One of the difficulties with a cyber intrusion is the immediate attribution. You do not know whether it is another government who is seeking to exfiltrate information from the national services or from the military or what have you. You don't know whether there is a group of individuals that have come together,

maybe a terrorist group, or a high school student across the street that is responsible for it.

We established several years ago the National Cyber Investigative Joint Task Force in which we, along with other members of the intelligence community, law enforcement community, have this task force in a separate place where we take each intrusion and immediately try to determine how best to investigate it, utilizing the capabilities of both the intelligence community, as well as the law enforcement community, and then investigate it either as a criminal threat or a counter-intelligence threat. So we are at the hub of the attribution and investigation side.

The Department of Homeland Security is responsible for alerting and protecting the private side of the Internet, and quite obviously, NSA and the new Cyber Command are responsible for protecting the Government entities, particularly when it comes to the military.

Mr. QUAYLE. So when you assess a threat and you determine whether it is criminal or whether it is more counter-intelligence, then criminal goes toward the FBI and counter-intelligence goes to——

Mr. MUELLER. It may well be but there may be——

Mr. QUAYLE. Some overlap?

Mr. MUELLER [continuing]. Expertise in any one agency. In other words, there may be expertise in the NSA. Ultimately it may turn out to be a criminal threat and we may want to go to court which requires different treatment. On the other hand, we may have expertise here that is helpful to the military. Or what happens more often than not in this day and again, it is cross-jurisdictional. The victims may be in the United States, the actors outside; or the actors in the United States and the victims outside. And consequently, the cyber threat, more than any other, because of the difficulty of attribution at the outset, requires us to work together in the task force concept to make certain that we gather all the information we can and then make a determination how best to address the threat whether it be through prosecution or through some sort of activity on the part of the intelligence community.

Mr. QUAYLE. When you were talking with Mr. Watt earlier, you were talking about IP theft that is pretty much rampant right now on the Internet, and you mentioned that the FBI had gotten increased funding in, I think it was, fiscal year 2009 and 2010 for specific agents that were specifically tasked with going into IP theft. There are reports out that there haven't been any increased investigations related to IP theft. And I would just want to know is it just because you are ramping up, or what is the reason that there is not increased investigations when more allocated resources have been given to the FBI?

Mr. MUELLER. Well, actually, we have over 460 investigations ongoing in intellectual property at this point in time. Some of them probably predated the addition of the 20 agents. And I would have to get back to you as to where they are and what particular investigations they are undertaking. But in the last year or so, we have undertaken a review to better allocate our resources to maximize the impact. But as I say, we have over 460 ongoing investigations. That is probably not enough given the extent of the crime out

there, but we have to prioritize and we do the best we can in terms of prioritizing.

Mr. QUAYLE. Okay, great. Thank you very much.

I yield back.

Mr. SMITH. Thank you, Mr. Quayle.

The gentleman from Florida, Mr. Deutch, is recognized.

Mr. DEUTCH. Thank you, Mr. Chairman.

Director Mueller, thank you for your service. I will be sorry to see you go this fall.

I want to get back to an exchange you had earlier with Mr. Conyers. Last year, the FBI had identified mortgage fraud as its most significant white-collar crime issue and noted that the number of investigations of mortgage fraud against financial institutions had been rising annually, and in fact, earlier this morning, you recited some statistics about the number of ongoing investigations.

Could you describe the results of those investigations thus far?

Mr. MUELLER. I think they have been very successful. I don't believe there is a month or 2 months that goes by without a substantial takedown of individuals who were involved in some sort of scheme relating to mortgage fraud. But I would have to get those statistics for you.

Mr. DEUTCH. I would appreciate that.

Mr. MUELLER. I think we have been quite successful and actually we have had a number of press conferences when we have taken down a number of particular cases around the country. So I will get you that information, sir.

Mr. DEUTCH. I appreciate that.

Does the FBI have sufficient resources to combat financial fraud and mortgage fraud?

Mr. MUELLER. We have over 3,000 mortgage fraud cases. We again do have to look at them through the working groups and the task forces that we have around the country. We try to make certain that we address each one either at the Federal level or at the State level. We have periodic reviews with each of our field offices at least twice a year in which I am asking about their mortgage fraud caseload and how they are addressing the mortgage fraud caseload and where the cases are in the course of investigation and prosecution, and if we can't do it, who is doing it. So I believe that has been successful in addressing this particular issue.

Mr. DEUTCH. As you do that analysis and make the determination that if you can't do it, who is doing it, what is the answer to that question that will satisfy you when you try to determine who else is doing——

Mr. MUELLER. If it is being addressed either by a local district attorney's office or in many cases the attorney general's office.

Mr. DEUTCH. Which then leads in to my next question. Beginning in the fall of last year when reports started to surface that certain mortgage services were submitting false, improper, or fraudulent court documents in support of foreclosure actions, there were reports that raised concern that the mortgage lending industry may have pursued—there may have been thousands of foreclosures unlawfully. At that time, the Justice Department indicated it was considering an investigation into whether there may have been criminal violations concerning the conduct of mortgage servicers.

If you could speak to the role of the FBI in the ongoing settlement talks and prosecutions, investigations surrounding the mortgage servicing industry specifically your interaction with, as you just pointed out, the State attorneys general in particular.

Mr. MUELLER. Our role would be to investigate allegations, accusations of illegal criminal activity in the mortgage services industry. I do believe we have ongoing investigations, but to the extent that there is discussion about settlements, it would be outside our realm. It would be the U.S. Attorney's office, the State attorney general, or other regulators.

Mr. DEUTCH. And just a change in direction, again this being your last time up here before the Committee. You touched briefly in your exchange with Mr. Quayle on some cyber issues. The Director of National Intelligence told the House Intelligence Committee last month that the cyber environment provides unprecedented opportunities for adversaries to target the U.S. due to our reliance on information systems.

If you could just speak to, one, whether you share Director Clapper's concern that the cyber environment presents these unprecedented opportunities for our adversaries and, two, whether you believe security of the system should be enhanced? Again, that is based on the investigations that the FBI may have been conducting addressing specifically the cyber security issues.

Mr. MUELLER. Well, I do agree with General Clapper. I think he is absolutely right in that the opportunities for intrusions and illegal cyber activity are growing exponentially as technology grows and that every one of us has an obligation to address security within their particular institutions or even within one's particular household. The Government as a whole, I know, is working. The Administration is working to continue to address this.

Our role, as I indicated before, is generally to investigate the intrusions and determine attribution, and then if it is someone over whom we have jurisdiction, to arrest, indict, and convict. We actually have had cases where we have had extradited from other countries persons who have undertaken illegal cyber activity and the victims are here in the United States. So not only is it a growing problem, it is a growing international problem where we cannot be content to reside in our own jurisdictions and just address what is happening in our jurisdiction because often the players, the actors are not in our jurisdiction but the victims may well be. So it will be a huge challenge in the future.

Mr. DEUTCH. Thank you, Director.

Mr. SMITH. Thank you, Mr. Deutch.

The gentleman from California, Mr. Gallegly, is recognized.

Mr. GALLEGLY. Thank you, Mr. Chairman.

Director Mueller, it is great to see you here this morning. You know, after just completing 8 years on Intel and seeing the diversity and the complexities of what you have to deal with every day, I have incredible respect for you and the job you have done. I have to say that I miss being on Intelligence, but there is an 8-year term limit. So we will find other challenges.

I know, as I was coming in this morning—and I was a few minutes late. But I know that there was some discussion as it relates to health care fraud. I recently had a group of folks from Los Ange-

les County's law enforcement agencies, county sheriffs, former DA's, and so on that had been working Medicare fraud in the greater Los Angeles area and in and around that regionally. It is mind-boggling to me the information that they passed on to me as it relates to Russian gangs, identity theft, and particularly with doctors, identity being taken and false claims being paid to doctors through these clinics that were using other doctors' names, and then these doctors not knowing about it until they get a letter from the IRS about not paying their income tax. I mean, it is a very complicated situation.

However, it gets beyond that. I would just like to maybe hear from you what your understanding of the depth of this problem is. I have had numbers that seem to be from credible sources that the fraud amounts on Medicare alone could be as much as $60 billion a year, which plays a major role in the success and the challenges of Medicare. Issues like women that are preyed on, particularly illegal immigrants, that are paid $25-$30 to go in and take mammograms two-three times a week and the concern, of course, on their health is an issue. Pharmacies that are selling three and four times as many drugs each week as they actually buy. So it is a revolving door where they are working in conjunction with some of these clinics that are nothing more than a computer front.

I just would like to know if you have some comments about how you are working with the identity theft and particularly the impact that it is having on Medicare.

Mr. MUELLER. I would hope that you had a briefing from a task force who is addressing it because in Los Angeles, as well as elsewhere, we address Medicare fraud, health care fraud together with State and local law enforcement.

One of the things you do point out which we have found recently is the intersection of organized crime with health care fraud. I would say there has been a substantial growth in the last 4 to 5 years of organized crime recognizing that health care fraud is a fertile field for activity. We had a series of arrests about a month, month and a half ago which laid out, at least, one substantial organized crime group that has spent substantial time and received substantial monies from Medicare fraud. So being aware of the intersection with organized crime is one aspect.

Another aspect is what you will find is if there is a scheme that has found a home in Tampa, which we identify and we prosecute and take down in Tampa, inevitably it will show up in Texas or Arizona or elsewhere. And so we have used the intelligence capabilities that we have developed frankly to address terrorism to make certain that we anticipate the schemes and prevent them from taking root elsewhere.

And so a combination of understanding the intersection with organized crime, the ability to try to get ahead of the scheme as it tries to take root elsewhere in the country, and lastly again I would go back to we cannot do this alone. It takes the combination of local district attorneys, State attorney general offices, as well as our agents and agents from the Postal Service, HHS, a number of the other agencies to work cooperatively in the task force or working group concept to address this particular threat.

Mr. GALLEGLY. One thing I asked, Director Mueller, was that it was represented to me that a major problem, at least in the greater Los Angeles area, are groups that are referred to as Russian gangs and there are other gangs. But is it your understanding that that is clearly a problem where a lot of the money is going offshore as they are getting it through these fraudulent ways here in the U.S.?

Mr. MUELLER. Let me just clarify one thing.

I would say more generally Eastern European, not just limited to Russia. Certainly Russian organized crime has been a player over the years, but the recent takedown, if I am not mistaken, was not Russia. It was an Eastern European country.

Mr. GALLEGLY. And a lot of that is going back. Money is going offshore.

Mr. MUELLER. Yes, absolutely.

Mr. GALLEGLY. Thank you very much, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Gallegly.

The gentlewoman from Florida, Ms. Wasserman Schultz, now serving as Ranking Member, is recognized for her questions.

Ms. WASSERMAN SCHULTZ. Nothing like going from last to first, Mr. Chairman. Thank you very much.

Director Mueller, it is good to see you again. Over the years, it has been a pleasure to work with you on the implementation of the Protect Our Children Act of 2008. I want to touch briefly on some of the issues surrounding that.

And I know Chairman Smith mentioned his concerns about data retention earlier in his questions. I share those concerns. And I want to make sure that we get some answers from you just to shed some light on the challenges that you face at the FBI and then within the larger Department of Justice. But I look forward to working with Chairman Smith on advancing a bipartisan bill that will help make sure that law enforcement can connect the dots when we are dealing with child exploitation investigations.

So the issue is that too many of these child exploitation investigations will go cold because of the lack of connectivity logs that link anonymous IP addresses to specific individuals that are often deleted by the time a criminal investigation ensues and the request is made. And it ranges from as small and as short as 7 days to as long as 90 days, but really that is an inadequate amount of time if the crime isn't discovered before that point.

So you had mentioned previously when I have asked you this before, but do you still favor giving law enforcement this additional tool to allow them to get access to those connectivity logs within a reasonable period of time?

Mr. MUELLER. Absolutely. It goes to the larger issue of records retention which is essential to our ability to conduct the types of investigations——

Ms. WASSERMAN SCHULTZ. Thank you.

And are you aware of cases that ran cold or that law enforcement ran up against dead ends because they couldn't get access to connectivity logs?

Mr. MUELLER. Yes.

Ms. WASSERMAN SCHULTZ. The law now has sort of a standard. Why is the preservation scheme under the Electronic Communications Privacy Act not strong enough currently?

Mr. MUELLER. It goes back to what you indicate. The connectivity logs would be an essential part of it, but email addresses, use of email address, past emails, past attachments that have crossed the Internet—that is the kind of records that would give us the capability to successfully conduct an investigation on an individual who is using every effort he or she can to avoid scrutiny by the authorities.

Ms. WASSERMAN SCHULTZ. Now, I have a very strong record on privacy going all the way back to Terry Schiavo. So it is hard to be second to me on the importance of privacy. But this is such a critical issue because for literally—I mean, we could say thousands of cases potentially go cold because of the lack of that access. Wouldn't it certainly be preferable for the industry to come up with their own uniform reasonable standard?

Mr. MUELLER. It would. In my mind there ought to be a dialogue with Congress with the private sector. You come up with a rational records retention policy. It used to be that storage was a problem, but with the advances in technology, I have not heard recently a company avert to storage as being a problem. But it is the privacy and the privacy interests in my mind can be protected adequately with a records retention policy that gives us the tools we need to conduct successful investigations.

Ms. WASSERMAN SCHULTZ. And the Chairman had the hearing with the industry here in which we indicated and urged them to please press forward on a voluntary standard. I am for making them do it if they don't do that.

But just last but not least, because I know we are pressing up against votes, how is the lack of predictable data retention by service providers a significant hindrance and even an obstacle in certain investigations? And can you give us some specific examples of cases that have gone cold because of the lack of access to that data?

Mr. MUELLER. Well, I can get back to you with cases where they have gone cold, but anybody that looks at it and compare it where we were when telephone toll records were readily available for years and years and years and you compare to—because the billing is so different at this juncture, there is no incentive for companies to keep these records. There has to be some mechanism that either voluntarily or mandatorily requires them to keep them.

Ms. WASSERMAN SCHULTZ. Just in closing, Mr. Chairman, I mean, we are literally jeopardizing children's lives by not having adequate access to this information, and I really look forward to working with you on making sure that we can get it.

Mr. SMITH. I agree. Thank you, Ms. Wasserman Shultz.

The gentleman from Pennsylvania, Mr. Marino, is recognized.

Mr. MARINO. Thank you, Mr. Chairman.

Good afternoon, Director. It is good to see you.

I think, as you know, I was a district attorney and a United States attorney, and I had the pleasure of working with the Bureau in many cases, and it was a distinct honor. And I want to compliment you and the Bureau because you certainly have significantly increased the effectiveness and efficiency and the prestige of the Bureau, and thank you for your work.

Mr. MUELLER. Thank you.

Mr. MARINO. Sir, I want to revert back a little bit here to the PATRIOT Act, the Senate's version that is coming up. The Senate bill requires a showing of specific facts for NSL's, national security letters, and 215 orders other than library and bookseller records. Has the term "specific fact" been defined by the FISA Court or by the Bureau?

Mr. MUELLER. No, I don't believe it has. You can read into it what you want. Again, my preference would be that the PATRIOT Act, as it sits, be reauthorized as it is now without the modifications or the insertion of, I would say, a somewhat confusing phrase to which you allude.

Mr. MARINO. Do you think that if the FBI is required to include a statement of specific facts, does it open up for interpretation by the Inspector General whether a particular set of facts was specific enough, and what problems would this cause the Bureau?

Mr. MUELLER. I think that is a possibility, although we work very closely with the Inspector General. I see what you are alluding to. I do think that is a possibility.

Mr. MARINO. Well, you have no reservations that something like that could be worked out, given the relationship that you have?

Mr. MUELLER. We would work through it if it were passed into law. Again, my preference would be that we have worked with these three provisions, and reauthorization of those three provisions would be appropriate in my mind. Adding additional provisions relating to the NSL's or something else would put it into different ball park.

Mr. MARINO. Thank you, and I yield back my time.

Mr. SMITH. Thank you, Mr. Marino.

We will now go to the gentleman from Texas, Mr. Gohmert, for his questions.

Mr. GOHMERT. Thank you, Mr. Chairman.

And thank you, Director. Nice to see you back.

You had mentioned earlier that—and it is in your written statement—the FBI has developed extensive outreach to Muslim communities. In an answer to an earlier question, I had understood you to say that Muslim communities were like all other communities. So I am curious, as a result of the extensive outreach program the FBI has had to the Muslim community, how has your outreach program gone with the Baptists and the Catholics.

Mr. MUELLER. I am not certain of necessarily the thrust of that question. I would say that our outreach to all segments of a particular city or county or society is good.

Mr. GOHMERT. Well, do you have a particular program of outreach to Hindus, Buddhists, Jewish community, agnostics, or is it just an extensive outreach program to——

Mr. MUELLER. We have outreach to every one of those communities.

Mr. GOHMERT. And how do you do that?

Mr. MUELLER. Every one of those communities can be affected by facts or circumstances——

Mr. GOHMERT. I have looked extensively and I haven't seen anywhere in anyone from the FBI's letters, information that there has been an extensive outreach program to any other community trying to develop trust in this kind of relationship. And it makes me won-

der if there is an issue of trust or some problem like that that the FBI has seen in that particular community.

Mr. MUELLER. I would say if you look at—one of our more effective tools are what we call "citizens academies" where we bring in individuals from a variety of segments of the territory in which the office operates and if——

Mr. GOHMERT. Okay. Well, Director, I have only got 5 minutes and so I need your answers to be very quick.

Mr. MUELLER. Look at the citizens academies, the persons there. They are a cross section of the community. They can be Muslim. They can be Indian. They can be Baptists.

Mr. GOHMERT. Okay, but no specific programs to any of those. You have extensive outreach to the Muslim community and then you have a program of outreach to communities in general is what it sounds like.

But let me ask you, are you aware of the evidence in the Holy Land Foundation case that linked the Council on American-Islamic Relations, CAIR, the Islamic Society of North America, and the North America Islamic Trust to the Holy Land Foundation?

Mr. MUELLER. I am not going to speak to specific information in a particular case. I would tell you, on the other hand, that we do not have formal——

Mr. GOHMERT. Are you aware of the case?

Mr. MUELLER. We do not have any formal relationship with CAIR because of concerns——

Mr. GOHMERT. Well, I have got the letter from the Assistant Director Richard Powers that says in light of the evidence, talking about during the trial evidence was introduced to demonstrate a relationship among CAIR, individual CAIR founders, including its current president emeritus and executive director and the Palestine Committee. Evidence was also introduced that demonstrated a relationship between the Palestine Committee and Hamas which was designated as a terrorist organization in 1995. In light of that evidence, he says the FBI suspended all formal contacts between CAIR and the FBI.

Well, now it was my understanding—and I have got documentation and I hope you have seen this kind of documentation before. It is a public record. And also the memo order from the judge is turning down a request that the unindicted co-conspirators be eliminated from the list. And he says the FBI's information is clear. There is a tie here and I am not going to grant the deletion of these particular parties as unindicted co-conspirators.

So I am a little surprised that you are reluctant to discuss something that has already been set out in an order, that has already been in a letter saying we cut ties in light of the evidence at this trial. I am just surprised it took the evidence that the FBI had being introduced at the trial in order to sever the relationships with CAIR that it had that showed, going back to a 1993 meeting in Philadelphia, was tied to a terrorist organization. So I welcome your comments about that.

Mr. MUELLER. Well, as I told you before, we have no formal relationship with CAIR because of concerns with regard to the national leadership.

Mr. GOHMERT. All right.

And are you familiar with the evidence from the Holy Land Foundation trial that showed that the founders of CAIR, Omar Ahmad and Nihad Awad, attended a mosque meeting in Philadelphia in 1993?

Mr. MUELLER. I am generally familiar with that case, sir.

Mr. GOHMERT. All right. Well, thank you. I see my time has run out.

One last question, though. Are you going to miss having to come testify at these Committees? [Laughter.]

Mr. MUELLER. That is the one question I will give a "no comment" to. [Laughter.]

Mr. SMITH. Thank you, Mr. Gohmert.

Director Mueller, thank you for your testimony today. Thank you for your 10 years of service as FBI Director and also for your many years of public service before that, including service in the military and your very distinguished career there as well. We very much appreciate it. We wish you well in your future endeavors too and appreciate all you have done.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witness and any additional materials for the record.

With that, we stand adjourned.

[Whereupon, at 12:11 p.m., the Committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the March 16, 2011, Hearing Before the House Committee on the Judiciary Regarding Oversight of the FBI

Questions Posed by Representative Scott

1. The FBI is very involved in investigating Medicare fraud. Please provide information about the amount of funds recovered vs. the cost of these investigations.

Response:

Through joint efforts by the Department of Justice (DOJ) and the Department of Health and Human Services (HHS), in Fiscal Year (FY) 2010 we recovered approximately $4 billion related to Medicare fraud. This represents an increase of approximately $1.47 billion, or 57 percent, over the amount recovered in FY 2009, which was itself a record amount. Indeed, over the past three years we have collectively recovered an average of nearly $7 for every dollar appropriated to support the costs of health care fraud investigation and prosecution.

In FY 2010, DOJ brought criminal health care fraud charges against 931 defendants, the most ever in a single fiscal year, and we obtained 726 convictions, which was also a record. The FBI continues to investigate nearly 2,600 cases of health care fraud. For example, in February 2011, the Medicare Fraud Strike Force, a partnership between DOJ and HHS, charged more than 100 defendants in nine cities, including doctors, nurses, health care companies, and executives, for their alleged participation in Medicare fraud schemes involving more than $225 million in false billing. By all accounts, this was the largest federal health care fraud takedown in history.

2. Please inform us as to any changes to the gun laws which you think would be beneficial from the standpoint of safety to the general public and your agents in the field.

Response:

These responses are current as of 7/5/11

The FBI would be pleased to provide its views of possible legislation on this topic to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position.

3. Please inform us as to any challenges presently faced by the FBI lab.

Response:

Like other FBI Divisions, the FBI's Laboratory Division (LD) has efficient systems in place and is able to address its challenges provided that it continues to be adequately resourced. The LD programs and capabilities that are most challenged by the possibility of inadequate resources are the Combined DNA Index System (CODIS), the Terrorist Explosive Device Analytical Center (TEDAC), and the Laboratory Information Management System (LIMS).

CODIS

CODIS is the software that manages the nation's DNA database. All levels of law enforcement depend on its functionality, capability, and dependability to assist in solving crimes and identifying individuals who pose a risk to our nation's security. The development of advanced technologies requires interoperability enhancements to the CODIS software to ensure CODIS' compliance with security, certification, and accreditation requirements. One of these technologies is the FBI's Rapid DNA Program, which will provide law enforcement agencies the ability to develop DNA profiles from arrested individuals during the booking process. This real-time match is designed to assist in preventing future crimes by expeditiously linking individuals to unsolved cases in which they were involved. The FBI also plans to continue the National Missing Person DNA Database Program (which processes mitochondrial and nuclear DNA related to missing persons and enters these profiles into CODIS) and to develop familial searching software (to identify close biological relatives of the source of a forensic sample associated with a crime scene).

TEDAC

TEDAC provides the ability to confirm the electronic characteristics of explosive devices, analyze and associate devices through tool marks, study explosive material through chemical analysis, provide latent fingerprint matching, and recover and compare trace evidence and DNA. TEDAC's functions are performed in a high-capacity, multi-agency, collaborative environment using

experienced and certified scientists, engineers, and technicians. These TEDAC functions include identifying associations between events, people, and improvised explosive devices using the full spectrum of technical and forensic techniques and equipment and conducting in-depth all-source analysis to ensure we fully understand the nature of the threat.

LIMS

The FBI is working to develop LIMS in order to automate the tracking and management of evidence to improve in-processing, storage, transfer, and inventory control. LIMS is designed to reduce or eliminate bottlenecks and to improve turnaround times in the processing of all types of evidence evaluated at the FBI's Laboratory.

4. There are proposals pending in Congress to cut various aspects of the FBI's budget. Please provide examples of the impact of cutting your resources? What aspects of your work are most likely to be reduced or eliminated if cuts are passed?

Response:

As with all federal departments and agencies, funding disruptions and hiring freezes have long-term impacts on the FBI. When hiring is frozen, candidates may seek other employment, and staffing reductions may affect mission performance. For example, in the past Congress has questioned the FBI's vacancies in mid-level manager positions. These vacancies were the direct result of hiring freezes in prior years, during which we would have brought on board the employees who would have filled these management positions in later years.

5. What could the FBI do with more agents regarding organized retail theft and ID theft?

Response:

The FBI works to combat both organized retail theft and identity theft. Agents working organized retail theft focus primarily on the interstate transportation of stolen property, collaborating with the retail industry, working with federal, state, and local law enforcement partners, and helping to develop the Law Enforcement Retail Partnership Network. As always, investigative resources affect how quickly, and how many, investigations are conducted. An increase in the agents working identity theft cases would allow us to establish an identity theft training program for our cyber agents, establish a working group to foster closer

coordination with industry, assign a full-time cyber agent to the Federal Trade Commission, and enhance the FBI's current system of tracking identity theft cases.

Questions Posed by Representative Pierluisi

The work of the Federal Bureau of Investigation is critically important to Puerto Rico. Far too many lives on the Island are lost each year to violent crime. While the overall U.S. homicide rate has declined substantially in recent decades, the number of murders committed in Puerto Rico has increased steadily. Last year, 983 murders were committed on the Island, up from 894 in 2009. For comparison, in New York, which has five times Puerto Rico's population, 778 murders were committed in 2009—approximately 200 fewer than were committed in Puerto Rico during the same time period. Regrettably, Puerto Rico serves as a key transit point for drugs produced in Central and South America and destined for consumption in the 50 states. The Puerto Rico Police Department has estimated that more than 75% of the murders in Puerto Rico are linked to this illegal drug trade, and anecdotal evidence suggests this figure may be a conservative estimate.

Last July, I wrote to Attorney General Holder, copying you, to request that the level of federal resources devoted to fighting violent crime in Puerto Rico be made commensurate with the Island's needs in this area. I had a productive meeting with the Attorney General last September; he pledged to work with me and the Puerto Rico government to devise new approaches to addressing drug-related crime on the Island. The Report by the President's Task Force on Puerto Rico's Status, issued on the same day as your testimony, echoed the Attorney General's commitment to solving Puerto Rico's crime problem. The Report recognized that Puerto Rico's high murder rate is a cause of significant concern on the Island, and recommended that a working group of federal security and law enforcement agencies be convened to determine how federal programs could be better leveraged to create a safer Puerto Rico.

Although I appreciate the sentiments offered by the Attorney General and in the Report, words are no substitute for action. I know you share my view that a murder in Puerto Rico is just as tragic as a murder in New York City or Chicago or Los Angeles.

6. What steps is the FBI taking to address drug-related violent crime in Puerto Rico?

Response:

These responses are current as of 7/8/11

Because the FBI considers Puerto Rico to be the "eastern flank" of its Southwest Border strategy, we have established one of our "hybrid" squads in Puerto Rico. Hybrid squads combine members of drug squads with members of gang squads and task force officers from state and local police departments to focus on the criminal activities of Mexican and other Latin American criminal enterprises, including the sale of illegal drugs and weapons.

In addition to the hybrid squad, the FBI uses four Violent Gang Safe Streets Task Forces (VGSSTFs) to combat violent crime in Puerto Rico: the San Juan Safe Streets Task Force, the Aguadilla Safe Streets Task Force, the Ponce Safe Streets Task Force, and the Fajardo Regional Enforcement Team. The VGSSTF concept expands cooperation and communication among federal, state, and local law enforcement agencies, increasing productivity and avoiding duplication of investigative efforts. One of the key facets of a VGSSTF investigation is the Enterprise Theory of Investigation (ETI). Combining short-term, street-level enforcement activity with sophisticated investigative techniques, such as consensual monitoring, financial analysis, and Title III wire intercepts, investigations using ETI work to root out and prosecute entire gangs, from street-level thugs and dealers, up through crew leaders, and ultimately including the gang's command structure.

7. How many full-time equivalent positions does the FBI assign to Puerto Rico?

Response:

Organizationally, FBI personnel are assigned to Divisions. One of these Divisions is the San Juan Division, which includes Puerto Rico. As of 3/31/11, 310 full-time Special Agents, Intelligence Analysts, and Professional staff positions were assigned to the San Juan Division.

8. How many of those positions are filled?

Response:

As of 3/31/11, approximately 93% of the positions in the San Juan Division were filled.

9. How do the numbers of assigned positions and filled positions compare with jurisdictions that are of a similar size and that have a similar murder rate as Puerto Rico?

Response:

In 2009 (the most recent year for which crime data are available), Puerto Rico had a population of approximately 4 million and a murder rate per 100,000 inhabitants of 22.5. The jurisdictions with the most comparable murder rates were the District of Columbia (with a population of approximately 600,000 and a murder rate of 24.0) and Philadelphia (with a population of approximately 1.5 million and a murder rate of 19.5). Unfortunately, funded staffing levels (FSLs) are assigned by Field Office rather than by city, and there is not a Field Office for Philadelphia, alone, or for Washington, D.C., alone (the agents assigned to those cities are responsible for far broader geographical areas than just those cities). Consequently, we are not able to compare the numbers of assigned and filled positions in Puerto Rico with those of comparable jurisdictions. Even if that were possible, though, we note that many factors are considered when establishing an office's FSL. For example, more agents might be assigned in a location such as Washington, D.C., than in another city with a comparable population because the nature of the location makes it a greater target for a variety of criminal activities. In addition, to the extent that the FBI might adjust FSL based on crime statistics, it would do so only based on crimes for which the FBI has jurisdiction. While this would include some murders, it would not include all murders, because murder is typically a state/local crime and is not investigated by the FBI unless a federal nexus exists.

10. What other resources has the FBI devoted to Puerto Rico?

Response:

In addition to the efforts discussed above, the FBI's San Juan Division works closely with the Policia de Puerto Rico (POPR) Strike Force, which is comprised of elite street gang units. Through its coordination with these units, the FBI has access to the POPR's intelligence, evidence, and potential human sources. In addition, approximately 60 former Strike Force agents who have returned to their police departments remain a significant source of intelligence regarding emerging threats. The FBI also involves its federal partners, including the Bureau of Alcohol, Tobacco, Firearms, and Explosives and Immigration and Customs Enforcement, in the investigative process as "force multipliers."

11. How does that level of resources compare with jurisdictions that are of a similar size and that have a similar murder rate as Puerto Rico?

Response:

As discussed in response to Question 9, above, the FBI's Field Offices are not aligned along city or other jurisdictional lines, and they are typically not aligned along state lines, so there is no easy way to identify what Field Offices are "of similar size" to Puerto Rico. The task forces and other force multipliers employed in the various FBI Field Offices share some common elements (such as the JTTFs, which operate in all FBI Field Offices), but the purposes and compositions of a Field Office's task forces are tailored to address the local law enforcement and national security challenges. Puerto Rico poses unique challenges because the majority of the violent crime problem stems from the fact that gangs have staked their claims to over 50 of the approximately 350 public housing projects on the island. In response, as discussed in response to Question 6, above, the FBI operates one hybrid squad and four VGSSTFs in Puerto Rico. By comparison, most FBI Field Offices have no hybrid squads and some have only one task force, while a few may have both a hybrid squad and multiple task forces, depending on the size of the Field Office and the crime and intelligence demands involved.

12. Are you confident that sufficient FBI personnel and resources are being devoted to Puerto Rico to successfully combat drug-related violence and achieve a reduction in the murder rate?

Response:

Although additional resources are always beneficial in combating crime, in light of the competing needs for these resources and the FBI's other priorities we believe the proper balance has been achieved. In Puerto Rico, the FBI uses task force officers from local and state law enforcement agencies extensively to provide continuity in operations and investigations. Continuity in operations and experience are key ingredients of successful strategies in addressing drug and violent crime problems, which are the primary contributors to a high homicide rate.

Questions Posed by Representative Quigley

Guns

13. The Mexican drug cartels are killing people at a staggering rate – more than 30,000 since 2006. According to the National Drug Intelligence Center, Mexican drug trafficking

organizations have infiltrated small and large cities in 48 U.S. states, affecting our national security.

For example, Mexican drug cartels have a significant presence in my home town of Chicago, which federal officials say is a key transfer point for drugs heading to Minnesota and points north and east.

The drug cartels are getting their guns from the United States.

Since 2006, the ATF has seized more than 10,000 firearms and nearly one million rounds of ammunition destined for Mexico, where the public is not allowed to purchase or possess guns.

I know we have many federal officials south of the border working to crackdown on these cartels. But in your opinion, is the trafficking of guns from the U.S. to Mexico a national security threat, and if so, what should be done to combat it?

Response:

The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) is DOJ's component with primary jurisdiction for combating the illegal flow of non-military firearms available at the retail level from the United States into Mexico and other Central and South American countries. The FBI defers to ATF to address inquiries regarding this transportation of weapons.

National Security Letters

14. Critics say that the NSL provisions should be amended so that they collect information only on suspected terrorists and the gag should be modified to permit meaningful court review for those who wish to challenge nondisclosure orders. What are your thoughts on these proposed improvements?

Response:

National Security Letters (NSLs) are used during national security investigations the same way grand jury subpoenas are used during traditional criminal investigations - to obtain information that can be used as the building blocks of an investigation. This information includes telephone toll records, banking records, and credit records. NSLs are a necessary and valuable investigative tool in national security investigations, including counterterrorism, espionage, and

counterintelligence investigations. Without this authority, the FBI would not be able to effectively protect the nation.

Meaningful court review is already provided by statute. Currently, an NSL recipient may disclose the existence of the NSL to an attorney to obtain legal assistance with respect to the request and may petition a federal court to modify or set aside a nondisclosure order.

Last year's OIG Audit on Foreign Translation Program

15. Regarding the foreign language translation program, the report states that the FBI had significant unreviewed electronic file material for cases in the two highest priority categories. It concluded that not reviewing such material increases the risk that the FBI will not detect information in its possession that may be important to its counterterrorism and counterintelligence efforts.

In a more global sense, the threat posed to us by terrorism presents a moving target and necessitates that we continually re-adjust resources and re-assess policies. In your opinion, would you conclude that the FBI has shown itself to be fluid in its policy and decision making, or does it appear slow or reticent to revise practices and protocols to meet the challenges posed by changing threats?

Response:

The FBI prioritizes its translation efforts based on the potential threat (terrorism, intelligence, or criminal) represented by each target. Threat levels are evaluated based on classified United States Intelligence Community standards. Consistent with the FBI's top priority of preventing terrorist attacks, it is the FBI's policy that all counterterrorism materials will be reviewed, regardless of age. Consistent with the FBI's established priorities, the review of counterintelligence materials receives a lower priority. While we recognize that there may be important information in these lower-priority counterintelligence materials, we believe our finite foreign language resources should be applied first to our highest priority collection, followed by our most recently collected materials in the lower priorities. Counterintelligence materials are prioritized according to the potential threat they address. Over many years of collecting, processing, and reporting on these types of targets, the FBI has learned that this intelligence is highly "perishable," meaning this information loses value very quickly. We recognize, though, that a portion of the information may be relevant or useful at some point

long after collection. Consequently, all of the collection is archived for later retrieval should subsequent reporting make that appropriate.

The FBI also implemented a Strategy Management System (SMS) to communicate the FBI's strategy, prioritize initiatives, identify each component's role in pursuing the strategy, and measure progress. The SMS ensures that we continue to adapt to the changing threat environment and that we direct our resources to our strategic mission and goals.

Additional information responsive to this inquiry is classified and was provided separately to the Committee on March 5, 2012.

PATRIOT Act - Roving Wiretaps

16. In a criminal investigation, once a wiretap is concluded the subject is notified within 90 days. In an intelligence investigation that is understandably not the case. In what situations should a suspect be informed that they were the subject of a section 206 investigation?

Response:

Section 206 of the USA PATRIOT Act allows the Government to continue "roving" electronic surveillance when a person who is already subject to electronic surveillance approved by the Foreign Intelligence Surveillance Court switches from one facility (e.g., a telephone associated with one service provider/telephone company) to a different facility associated with a different provider. Courts have expressly rejected the argument that roving electronic surveillance violates the Fourth Amendment.

National security investigations that employ "roving" surveillance often involve highly trained foreign intelligence officers operating in the United States or terrorists who are skilled at trying to evade electronic surveillance. The FBI does not anticipate notifying such investigative subjects.

PATRIOT Act - Lone Wolf

17. Do you believe that the government would not be able to effectively investigate terror plots if the Lone Wolf power lapsed? Would other tools be available?

Response:

In today's environment of "self-radicalization" and easily accessible Internet content regarding terrorist recruitment and training, the availability of the "lone wolf" authority is vital to our efforts to prevent terrorist attacks. While Title III electronic surveillance may be an option, it is often not the best option because Title III does not provide the same ability to protect critical intelligence sources and methods as is offered by the "lone wolf" provision of the Foreign Intelligence Surveillance Act. If the lone wolf provision were to lapse, the government might be required to choose between stopping a current terrorist act and protecting the sources and methods that will be used to thwart future attacks.

Mattachine Society (LGBT Issue)

18. I would like to ask you about the results of some troubling FOIA requests some of my constituents have made on the Mattachine Society. As you may know, the Mattachine Society was one of the earliest homophile organizations in the United States. Through a FOIA request, the FBI released a lengthy file it kept on the Mattachine Society.

However, other FOIA requests on LGBT individuals were made to which the FBI states that the records "are currently unavailable" and "palletized and designated for shipment to the National Archives." However, the National Archives has stated that these file numbers are still in the physical and legal custody of the FBI.

So the question we are trying to answer is, first, is where are the files? Unfortunately, these specific requests to the FBI have resulted in dead ends. I understand that you may not have this information at your disposal now, but if you could have your staff look into it, I would be greatly appreciative.

Response:

Since January 2010, the FBI has been preparing eligible Domestic Security files for transfer to the National Archives and Records Administration (NARA). Case files that have been closed for a minimum of twenty-five years are being reviewed, inventoried, boxed, palletized, and shipped to NARA. When the FBI transfers physical custody of a record to NARA, the FBI's tracking system is updated to indicate that the record is at NARA. It is the FBI's understanding that, if NARA receives a FOIA request for records that are on pallets awaiting transfer, NARA places the request in its FOIA queue. This ensures the requestor will not lose its place in the assignment queue as a result of the record transfer. Often the record transfer will have been completed by the time the request reaches the front

of the NARA queue. As to the "other FOIA requests on LGBT individuals," we would need to know the names of the subjects of the requests to identify the locations of the responsive records.

○