Department of Justice

STATEMENT FOR THE RECORD OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

JULY 28, 2010

Statement of Robert S. Mueller, III
Director
Federal Bureau of Investigation
Before the Senate Judiciary Committee
"Oversight of the Federal Bureau of Investigation"
July 28, 2010

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

Since the Committee's last oversight hearing, the FBI has faced an extraordinary range of national security and criminal threats. There was the plot to bomb the New York City subway system exemplifying how core al Qa'ida remains committed to attacking America. There was the attempted airline bombing on Christmas Day directed by al Qa'ida in the Arabian Peninsula (AQAP) and the attempted car bombing in Times Square aided by Tehrik-e-Taliban in Pakistan (TTP), demonstrating how al Qa'ida affiliates also have the intent to strike inside the United States.

There were the arrests 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 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 corporate and mortgage frauds, involving massive Ponzi schemes and sophisticated insider trading, 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. And throughout, there were serious corruption cases that undermined the public trust, and violent gang cases that continued to endanger our communities.

These examples underscore the complexity and breadth of the FBI's mission to protect the nation in a post-9/11 world. They also demonstrate how the FBI has evolved as a threat-based, intelligence-driven agency in responding to these threats, and how the FBI will meet these challenges in the years to come.

Let me discuss a few of these examples in my testimony today.

Counterterrorism

Terrorism, in general, and al Qa'ida and its affiliates, in particular, continue to represent the most significant threat to our national security. As we have seen over the past year, al Qa'ida and its affiliates remain committed to conducting attacks inside the United States, and they constantly develop new tactics and techniques in an attempt 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.

In response, the FBI has drawn on the full range of its counterterrorism tools, both at home and abroad, to meet these new and existing threats. Last fall, the FBI disrupted the al Qa'ida plot of Najibullah Zazi and others who were planning to attack the New York subway system. On December 25, 2009, Umar Farouk Abdulmutallab attempted to bomb Northwest Airlines Flight 253, an attack directed by elements of AQAP. In May, Faisal Shahzad attempted to detonate a car bomb in Times Square, an attack linked to support from the TTP. Within days of the Christmas Day attack, the FBI established a Yemen fusion cell to coordinate our intelligence and counter-terrorism assets in response to AQAP. The FBI has similar groups focused on the Afghanistan-Pakistan region and on al Shabaab. After their arrests, the FBI has repeatedly debriefed Zazi, Abdulmutallab, and Shahzad. Additionally, the FBI's forensics and technical experts developed crucial evidence aiding these fast moving terrorism investigations. Equally important, the intelligence gained from these investigations, including the debriefings of these individuals, was voluminous and significant, and shared expeditiously with our domestic and foreign partners.

Earlier this month, al-Shabaab took credit for detonating two bombs in the Uganda capital of Kampala, killing more than 70 people including an American. In response, the FBI deployed more than 50 forensic and counterterrorism experts to Uganda to assist in the investigation of the blasts in Kampala. This effort is part of the FBI's long-term commitment to assist in significant terrorism investigations world-wide, as well as our focus to obtain intelligence and evidence in response to any threat from al Shabaab in the United States and overseas.

Homegrown and "lone wolf" extremists also pose a serious threat along with traditional international terror groups. We saw attacks on the military and its facilities in the United States with the Fort Hood killings in November and the Arkansas recruitment station shootings just over a year ago. There were also attacks on commercial and government targets with the disruption of the attempted bombings of an office tower in Dallas, Texas and a federal building in Springfield, Illinois. U.S.-born extremists also plotted to commit terrorist acts overseas, as was the case with the armed Boyd conspiracy in North Carolina, and David Headley's involvement in the Mumbai attacks.

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.

Counterintelligence

The foreign intelligence threat to the United States continues unabated, as foreign powers compete with the United States in economic, military, and diplomatic arenas. As we saw with the recent arrest of a network of ten Russian spies, foreign intelligence services remain active and aggressive in the United States.

The Russian "illegals" spy case demonstrates the long-term commitment of our adversaries. Sent here over the past two decades, the Russian agents took on the appearance of average Americans, in many cases adopting fake "legends" as United States citizens, obtaining work, and settling into quiet, family lives. These agents received hundreds of thousands of dollars in cash from their handlers to maintain their secrecy in America, even as they communicated through encrypted radio bursts and steganography posted in photos on the Internet. While these agents were in the United States, the FBI tracked their movements, activities, and intentions up until the time of their arrests.

Similarly, the conviction of Cuban spies Walter Meyers, a former State Department official, and his wife, offer similar counterintelligence lessons. Myers and his wife were recruited by the Cubans in the late 1970s and passed classified information to the Cubans for 30 years. Within the last month, Myers was sentenced to life imprisonment for his crimes; his wife received a sentence of nearly 7 years.

These cases reinforce how 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 exclusively on such traditional agent networks, as they increasingly employ non-traditional collectors—such as students, visiting scientists, scholars, and businessmen—as well as cyber-based tools to target and penetrate United States institutions.

To counter this threat, the FBI relies on its traditional counterintelligence programs and methods, but also has developed the National Strategy for Counterintelligence to deter and disrupt the modern counterintelligence threats. Its success relies heavily on strategic partnerships to determine and safeguard those technologies which, 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 community partners are able to identify and effectively protect projects of great importance to the U.S. government.

Cyber Security

The cyber threat to national security remains among our highest priorities. As the Committee knows, a cyber attack could have the same impact as a well placed bomb. To date, terrorists have not used the Internet to launch a full-scale cyber attack, but other criminal groups have executed numerous denial-of-service attacks and defaced websites, including an incident involving Congressional websites following President Obama's State of the Union address.

In the past ten years, al Qa'ida and its affiliates have created a potent online presence. Extremists are not limiting their use of the Internet to radicalization; they are using it to propagate terrorism, as we saw with the arrest of Colleen LaRose, known as "Jihad Jane", who has been charged with using the Internet to recruit jihadists and solicit funds for terrorists.

In addition to the terrorist threat, the Internet has been used as a means of attack for political ends. We saw this with the cyber attacks in Estonia in 2007 and in Georgia in 2008 that shut down banks and emergency phone lines, gas stations and grocery stores, and even parts of their governments.

As with the Google intrusion earlier this year, the cyber threat is focused on Internet businesses, and even individual users. Internet fraud and identity theft remain a growing problem, as the Internet Crime Complaint Center ("IC3") reported a 22 percent increase in reported offenses with more than 330,000 complaints involving more than $550 million in losses. These cyber incidents and frauds undermine the integrity of the Internet, threatening the privacy and pocketbooks of all who use it. Of course, finding, arresting, and punishing those who use the Internet to conduct sexual exploitation crimes remains among our highest responsibilities.

The FBI's response to these threats begins with our cyber squads in each of our 56 field offices with more than 1,000 specially trained agents, analysts, and digital forensic examiners. The FBI has also led the development of the National Cyber Investigative Joint Task Force ("NCIJTF"), which now includes 17 intelligence and law enforcement partners, working side-by-side to identify the source of national security threats and significant internet schemes. In support of victims of internet crime, the FBI has expanded the IC3, which continues to receive, track, and refer for prosecution the ever-increasing wave of internet crimes from child exploitation to fraud. Of course, the FBI remains committed to pursuing online sex offenders through the Innocent Images National Initiative and our long-standing cooperation with the National Center for Missing and Exploited Children. With these efforts, the FBI is committed to working with all our state, local, federal, foreign, and private partners in response to the cyber threats we face today.

Financial Crimes

Financial crimes ranging from major mortgage and corporate frauds to the scourge of large-scale health care frauds continue to pose a significant threat to our nation's financial and health care systems. Of course, these frauds directly victimize millions of homeowners, shareholders, and those seeking health care.

The FBI continues to uncover massive frauds and Ponzi schemes in the wake of the financial crisis. In June, Lee Bentley Farkas, former chairman of Taylor, Bean, and Whitaker, was charged with a $1.9 billion fraud that contributed to the failure of Colonial Bank, one of the 50 largest banks in the United Sates. Just this month, Nevin Shapiro, owner and former chief executive officer of Capitol Investments, was charged in an $880 million Ponzi scheme involving his firm in New Jersey. Over the past four months, the prosecutions of the Galleon insider trading case in New York and the Petters $3.9 billion Ponzi scheme in Minnesota continued with guilty pleas and significant sentences of top-level corporate executives. These cases are just a few examples from the thousands of mortgage and corporate fraud investigations ongoing at the FBI and in conjunction with the Administration's Financial Fraud Enforcement Task Force.

The FBI currently has 23 Mortgage Fraud Task Forces and 67 Mortgage Fraud Working Groups nationwide. With representatives of federal, state, and local law enforcement, the task forces are strategically placed in locations identified as high threat areas for mortgage fraud. The FBI has also created the National Mortgage Fraud Team (NMFT), at FBI Headquarters in Washington, D.C., which oversees the FBI's Mortgage Fraud Program. Through program guidance, oversight, training, and information sharing, the NMFT provides the tools necessary to identify

the most egregious mortgage fraud perpetrators and to prioritize pending investigations, as the FBI uses its resources as effectively as possible to combat mortgage fraud.

The focus on health care fraud is no less important. In May 2009, Attorney General Eric Holder and Health and Human Services (HHS) Secretary Kathleen Sebelius announced the creation of the Health Care Fraud Prevention and Enforcement Action Team (HEAT) and renewed their commitment to fighting health care fraud as a Cabinet-level priority at both departments. The FBI is a key component of the HEAT's efforts. Just two weeks ago, the Medicare Strike Force in Miami, Baton Rouge, Brooklyn, Houston, and Detroit announced charges against 94 individuals involved in more than $251 million in alleged false claims to federal health care programs. These charges involved fraud schemes that continue to plague the Medicare system related to billing for physical therapy, occupational therapy, home health care, durable medical equipment, and HIV infusion treatments. The FBI has partnered with investigators from the Department of Health and Humans Services, as well as other federal and state partners, in Medicare Fraud Strike Forces across the country, which have been expanded in connection with the HEAT initiative. In the past few years, the number of pending FBI health care fraud investigations has steadily increased to more than 2,500 cases. In the past 18 months, more than 1,600 defendants have been charged at both the federal and state level and more that 1,100 defendants have been convicted in these health care fraud investigations

Public Corruption

The FBI also recognizes that fighting public corruption is vital to preserving public confidence in government, protecting our borders, and securing our communities. In the past year, the FBI has led a number of long-term government and police corruption investigations in New Jersey, Louisiana, and other states that have uncovered significant political and official corruption. In the past two years, the FBI has contributed to the successful prosecution of approximately 1,600 federal, state, and local officials in corruption matters which were prosecuted in both federal and state courts throughout the country. Another 3,200 public corruption investigations are pending, approximately 2,500 of which involve public officials.

The Southwest border is a particular focus of the FBI's anti-corruption efforts. The FBI currently has approximately 145 agents assigned to twelve border corruption task forces along the Southwest border. The FBI has joined with our federal partners in these task forces, including the Department of Homeland Security Office of Inspector General, Customs and Border Protection Internal Affairs, Transportation Security Administration, the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and the U.S. Immigration and Customs Enforcement - Office of Professional Responsibility. To date, this collaboration has resulted in more than 400 public corruption cases originating from that region, with over 100 arrests and 130 state and federal cases prosecuted in fiscal year 2009. In addition, these border corruption task forces share information with the Southwest Intelligence Group, the El Paso Intelligence Center, and Mexican legal attachés to both identify and disrupt Mexican drug trafficking organizations from using U.S. public officials to facilitate criminal activities.

Since the inception of Operation Enduring Freedom in Afghanistan in 2002, the United States Government has privatized hundreds of functions that were previously conducted by military

personnel. While the vast majority of these contractors operate within the law, there has been an emergence of complex and wide-ranging contractor fraud schemes in Iraq, Afghanistan and Kuwait. To combat these fraud schemes, in 2006 we joined with our partners in standing up the International Contract Corruption Task Force (ICCTF), which falls within the mission and charter of the Department of Justice's National Procurement Fraud Task Force. Moreover, in 2007, we established a Joint Operations Center (JOC), which is overseen by the International Corruption Unit (ICU) and staffed by representatives of all nine Task Force agencies. The JOC ensures standardization of operation and real-time sharing of information, and agency representatives work to de-conflict investigations, and to support operations overseas. Since 2004, the Task Force has initiated nearly 700 investigations in Afghanistan, Iraq, and Kuwait with 273 currently open and pending. During this same time period, Task Force investigations have obtained over $47 million in restitution orders and $1 million in forfeitures/seizures.

The Civil Rights Unit has continued its work on a number of extremely important cases. For example, five former New Orleans police officers pleaded guilty to conspiring to manufacture a story to cover-up the wrongful killing of two and wounding of four at the Danziger Bridge just after Hurricane Katrina, and six other officers were indicted on July 13 for their roles as shooters or conspirators. On June 28, former Chicago Police Department Commander Jon Burge was convicted on perjury and obstruction charges related to his denials that he participated in the torture of suspects in police custody decades ago. And on June 4, a husband and wife were sentenced for their roles in forcing a Nigerian widow to perform domestic labor for them for more than eight years. Additionally, we continue to devote significant resources to investigate approximately fifty unsolved Civil Rights era homicides pursuant to the Emmett Till Unsolved Civil Rights Crime Act of 2007.

Gangs/Criminal Enterprises

From a national perspective, the FBI focuses its efforts on the most violent and dangerous gangs who present the greatest threat to our communities. Since the FBI's establishment of the Safe Streets Violent Crimes Initiative in 1992, the FBI has focused on violent gangs by identifying and targeting major groups acting as significant criminal enterprises. By conducting multi-subject and multi-jurisdictional investigations, the FBI concentrates on the worst gangs involved in a pattern of racketeering and those most difficult to prosecute, such prison gangs and those based overseas. This investigative model enables the FBI to target senior gang leadership and develop enterprise-based prosecutions.

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

In March, more than 200 federal, state and local law enforcement personnel participated in Operation Knock Down. Approximately 100 members and associates of Barrio Azteca were targeted in order to generate leads regarding the ongoing investigation in the Juarez murders, to

disrupt Barrio Azteca activities, and to gain valuable intelligence about the gang. This operation has contributed to recent arrests of senior leaders of the gang in Mexico, including those believed to be involved in the U.S. consulate employee murders.

Indian Country

The FBI has the primary federal law enforcement authority for felony crimes in Indian Country. Even with demands from terrorism and other threats, Indian Country law enforcement remains a priority for the FBI. The FBI's Safe Trails Task Force initiative -- which focuses entirely on Indian Country crime -- has grown steadily since its inception in 1994. There are now 19 Safe Trails Task Forces operating in Indian Country, and the FBI remains committed to working with its state and tribal partners in combating Indian Country crime.

In addition, the FBI's Indian Country Special Crimes Unit works with the Bureau of Indian Affairs to sponsor and promote core training for investigators. Each year, the FBI provides more than 20 training conferences for local, tribal, and federal investigators regarding gang assessment, crime scene processing, child abuse investigations, forensic interviewing of children, homicide investigations, interviewing and interrogation, officer safety and survival, crisis negotiation, and Indian gaming. Furthermore, the FBI's Office for Victim Assistance dedicates 31 Victim Specialists to Indian country, representing approximately one-third of the entire FBI Victim Specialist workforce.

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 new and old challenges. I look forward to working with the Committee in the future 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.