Department of Justice

STATEMENT OF

ROBERT S. MUELLER III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE

REGARDING

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

PRESENTED

DECEMBER 14, 2011

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

Introduction

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

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

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

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

Counterterrorism

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

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

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

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

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

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

Counterintelligence

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

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

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

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

Cyber Intrusions

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

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

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

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

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

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

Financial Crimes

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

Corporate and Securities Fraud

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

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

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

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

Health Care Fraud

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

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

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

Mortgage Fraud

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

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

Public Corruption

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

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

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

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

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

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

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

Gangs/Violent Crime

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

Violence Along the Southwest Border

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

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

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

Organized Crime

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

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

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

Crimes Against Children

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

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

Indian Country

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

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

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

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

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

Future Challenges

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

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

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

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

Conclusion

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