Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

MAY 16, 2012

Statement for the Record
Robert S. Mueller, III
Director
Federal Bureau of Investigation

Committee on the Judiciary
United States Senate

Oversight of the Federal Bureau of Investigation
May 16, 2012

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.

As you know, the Bureau has undergone unprecedented transformation in recent years. Since the attacks of September 11th, we have refocused our efforts to address and prevent emerging terrorist threats. The terrorist threat is more diverse than it was 10 years ago, but today, we in the FBI are better prepared to meet that threat.

We still confront traditional espionage and work diligently to prevent foreign intelligence agents from gaining our nation's political, military or economic secrets.

We also face increasingly complex threats to our nation's cyber security. Nation-state actors, sophisticated organized crime groups, and hackers for hire are stealing intelligence and national security data, as well as trade secrets and valuable research from America's companies, universities, and government agencies. These cyber threats are also a risk for our nation's critical infrastructure.

Yet national security is not our only concern, as we remain committed to our criminal programs. In the economic arena, investment fraud, mortgage fraud, securities fraud and health care fraud have harmed the world's financial system and victimized investors, homeowners, and taxpayers.

And although crime rates may be down nationwide, gang violence still plagues many neighborhoods, and our communities continue to confront violent crime, crimes against children, and threats from transnational organized crime.

As national security and criminal threats continue to evolve, so too must the FBI change to counter those threats. We must continue to use intelligence and investigative techniques to find and stop criminals and terrorists before they act. As we face greater challenges, we in the Bureau are relying on our law enforcement and private sector partners more than ever before.

The FBI remains firmly committed to carrying out our mission while protecting the civil liberties of the citizens we serve.

Counterterrorism

Counterterrorism remains our top priority.

In the past decade, Al Qaeda has become decentralized, but the group remains committed to high-profile attacks against the West. We confirmed this with records seized from Osama bin Laden's compound just over a year ago, as well as the recent conviction of an Al Qaeda operative plotting to conduct coordinated suicide bombings in the New York City subway system.

Al Qaeda affiliates and adherents, especially Al Qaeda in the Arabian Peninsula (AQAP), currently represent the top counterterrorism threat to the nation. These groups have attempted several attacks in and on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

We also remain concerned about the threat from homegrown violent extremists. Over the last two years, we have seen increased activity among extremist individuals. These individuals have no typical profile; their experiences and motives are often distinct. But they are increasingly savvy and willing to act alone, which makes them difficult to find and to stop.

For example, in February 2012, the FBI arrested Amine El Khalifi, a 29-year-old Moroccan immigrant, for allegedly attempting to detonate a bomb in a suicide attack on the U.S. Capitol. According to court documents, Khalifi believed he was conducting the terrorist attack on behalf of al Qaeda, although he was not directly affiliated with any group.

Another example is the case of Rezwan Ferdaus, a 26-year-old U.S. citizen and graduate student residing in Ashland, Massachusetts. Last fall, Ferdaus allegedly planned to use unmanned, remote-controlled aircraft to attack locations in Washington, D.C., including the U.S. Capitol and the Pentagon. Ferdaus was influenced by radical websites advocating violent extremism, among other things, and had expressed admiration for Al Qaeda's leaders, but was not directly affiliated with any group. He had allegedly become extremist 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.

Much like every other multi-national organization, terrorist groups are using the Internet to grow their business and to connect with like-minded individuals. Al Qaeda uses online chat rooms and web sites to recruit and radicalize followers to commit acts of terrorism. AQAP has produced a full-color, English language online magazine. Cases such as these illustrate why we in the Intelligence Community must continue to enhance our intelligence capabilities and to share information to ensure that critical information gets to the right people – before any harm is done. The FISA Amendments Act (FAA), allows the Intelligence Community to collect vital

information about international terrorists and other important targets overseas while providing a robust protection for the civil liberties and privacy of Americans. I join the Attorney General and the Director of National Intelligence in urging Congress to reauthorize this authority before it expires at the end of this year.

The Bureau itself has established a Countering Violent Extremism (CVE) Office within the National Security Branch (NSB) to improve our effectiveness in empowering our state, local, and community partners to assist in this effort. The duties and goals of this office include developing a better understanding of, and countering the threat of, violent extremism in the United States, strengthening community partnerships and providing to state and local officials and to community leaders unclassified briefings regarding the threat of extremism, addressing CVE-related operational and mission-support needs, including investigations, analysis, and training, and coordinating Bureau interests with regard to CVE matters with those of other agencies to ensure U.S. Government efforts are aligned.

Counterintelligence

We still confront traditional espionage – spies working under diplomatic cover, or even posing as ordinary citizens.

Today's spies are also students, researchers, businesspeople, or operators of "front companies." And they seek not only state secrets, but trade secrets, research and development, intellectual property, and insider information from the federal government, U.S. corporations, and American universities.

Consider the recent case of Stewart David Nozette, a scientist who once worked for the Department of Energy, the Department of Defense, NASA, and the National Space Council. He was sentenced in March to 13 years in prison for attempted espionage, conspiracy to defraud the United States, and tax evasion after providing classified information to an undercover FBI agent whom he believed to be an Israeli intelligence officer.

In another case, Hanjuan Jin, a former software engineer at Motorola, Inc., was found guilty in February on charges of stealing the company's trade secrets. She was stopped by U.S. customs officials in February 2007 at Chicago's O'Hare International Airport with more than 1,000 electronic and paper proprietary documents from Motorola. She was attempting to travel on a one-way ticket to China. Authorities also recovered multiple classified Chinese military documents that described telecommunication projects for the Chinese military.

In another case, 36-year DuPont employee, Tze Chao, pled guilty in March to providing trade secrets concerning DuPont's proprietary titanium dioxide manufacturing process to companies controlled by the Chinese government. He admitted providing information he understood to be secret to DuPont and not available to the public. He faces up to 15 years in prison and a $500,000 fine plus restitution.

These cases illustrate the growing scope of the "insider threat" — when employees use their legitimate access to steal secrets for the benefit of another company or country.

Cyber

The counterintelligence threat is quickly becoming cyber-based. So much sensitive data is stored on computer networks, our adversaries often find it as effective, or even more effective, to steal vital strategic and economic information through cyber intrusions, rather than through more traditional human spies.

The cyber threat has evolved significantly over the past decade. Indeed, we anticipate that cyber security may become our highest priority in the future.

Foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate important government and military information, as well as valuable commercial data — information that can compromise national security as well as improve the competitive advantage of state-owned companies.

Unlike state-sponsored intruders, hackers for profit do not seek information for political power; rather they seek information for sale to the highest bidder. Some of these once-isolated hackers have joined forces to create criminal syndicates. Organized crime in cyber space offers a higher profit with a lower probability of being identified and prosecuted.

Additionally, hackers and hacktivist groups such as Anonymous and Lulz-Sec are pioneering their own forms of digital anarchy.

The end result of these developments is that we are losing data, money, ideas, and innovation. And as citizens, we are increasingly vulnerable to losing our personal information.

We in the FBI have built up an expertise to address these threats, both here at home and abroad.

We have approximately 70 cyber squads across our 56 field offices, with more than 1,000 specially trained agents, analysts, and forensic specialists. The FBI also has 63 Legal Attaché offices that cover the globe. Together with our international counterparts, we are sharing information and coordinating investigations. We have Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players.

Here at home, the National Cyber Investigative Joint Task Force brings together 20 law enforcement, military, and intelligence agencies to investigate current and predict future attacks. With our partners at DOD, DHS, CIA, and the NSA, we are targeting the cyber threats that face

our nation. The Task Force operates through Threat Focus Cells – specialized groups of agents, officers, and analysts that are focused on particular threats, such as botnets.

Together with our intelligence community and law enforcement agency partners, we are making progress toward defeating the threat – through our use of human sources, technical surveillance, and computer science.

Last April, with our private sector and law enforcement partners, the FBI dismantled the Coreflood botnet. This botnet infected an estimated two million computers with malware that enabled hackers to seize control of the privately owned computers to steal personal and financial information.

With court approval, the FBI seized domain names and re-routed the botnet to FBI-controlled servers. The servers directed the zombie computers to stop the Coreflood software, preventing potential harm to hundreds of thousands of users.

In another case, last fall we worked with NASA's Inspector General and our partners in Estonia, Denmark, Germany, and the Netherlands to shut down a criminal network operated by an Estonian company by the name of Rove Digital.

The investigation, called Operation Ghost Click, targeted a ring of criminals who manipulated Internet "click" advertising. They redirected users from legitimate advertising sites to their own advertisements and generated more than $14 million in illegal fees. This "click" scheme impacted more than 100 countries and infected four million computers, half a million of which were here in the United States.

We seized and disabled rogue servers, froze the defendants' bank accounts, and replaced the rogue servers with legitimate ones to minimize service disruptions. With our Estonian partners, we arrested and charged six Estonian nationals for their participation in the scheme.

Together with our partners at DHS and the National Cyber-Forensics Training Alliance, we are using intelligence to create an operational picture of the cyber threat to identify patterns and players, to link cases and criminals.

We must continue to share information with our partners in law enforcement, in the Intelligence Community, and in the private sector.

We also must segregate mission-centric data from routine information. We must incorporate layers of protection and layers of access to critical information. And when there is a compromise, we must limit the data that can be gleaned from it.

Attribution is critical to determining whether an attack on a U.S. company is perpetrated by a state actor, an organized criminal group or a teenage hacker down the block. We can use the ability to attribute an attack to a specific attacker to help deter future attacks.

We cannot simply minimize vulnerabilities and deal with the consequences. Collectively, we can improve cyber security and lower costs with systems designed to catch threat actors, rather than simply to withstand them.

Financial Crimes

We have witnessed an increase in financial fraud in recent years, including mortgage fraud, health care fraud, and securities fraud.

Mortgage Fraud

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. At the end of last year, the FBI had nearly 2,600 mortgage fraud investigations nationwide — and a majority, over 70 percent, of these cases included losses greater than $1 million dollars.

With the collapse of the housing market, we have seen an increase in schemes aimed at distressed homeowners, such as loan modification scams and phony foreclosure rescues. So-called "rescue services" claim they can expose errors by lenders that might allow owners to keep their homes. In reality, they are just a clever way to lure nervous consumers into giving up sensitive personal information and paying thousands of dollars in fees for false hopes. Indeed, in some cases, these criminals convince homeowners to sign away the deeds to their homes.

Other criminals preyed on investors' hopes of cashing in before the housing bubble burst. In March, 61-year-old Andrew Williams, Jr., of Hollywood, Florida, was sentenced to 150 years in prison for his role in a $78 million mortgage fraud scheme. Through the scheme, Williams promised to pay off homeowners' mortgages in five to seven years following an initial investment of $55,000. Unfortunately for investors, this was no more than a Ponzi scheme. Those who paid the fee and joined the "Dream Homes Program" later found that there was no money left to fund their mortgage payments.

The FBI has made mortgage fraud a top priority, because we recognize its negative impact on homeowners, neighborhoods, and our nation's economy.

Over the past four years, we have nearly tripled the number of Special Agents investigating mortgage fraud. Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud.

We also work closely with the Department of Housing and Urban Development's Office of Inspector General, U.S. Postal Inspectors, the IRS, the FDIC, SIGTARP, the U.S. Trustee Program, the Federal Housing Finance Agency's Office of Inspector General, the Federal Trade Commission, and the Secret Service, as well as with state and local law enforcement offices.

Health Care Fraud

Health care spending currently makes up about 18 percent of our nation's total economy and continues to rise. These large amounts of money present an attractive target for criminals — so much so that we lose tens of billions of dollars each year to health care fraud.

In February, the Medicare Fraud Strike Force – a partnership between the Department of Justice and the Department of Health and Human Services – broke up the largest alleged home health care fraud scheme ever committed.

Dr. Jacques Roy, the owner of Medistat Group Associates in the Dallas area, was arrested along with several others for allegedly billing nearly $375 million in fraudulent Medicare and Medicaid claims for home health care services. Between January 2006 and November 2011, Medistat had more purported patients than any other medical practice in the United States – including more than 11,000 patients from more than 500 home health agencies.

Since their inception in March 2007, Medicare Fraud Strike Force operations have charged more than 1,300 individuals who collectively have falsely billed the Medicare program for more than $4 billion. Recently, a nationwide takedown by Medicare Fraud Strike Force operations in seven cities resulted in charges against 107 individuals, including doctors, nurses and other licensed medical professionals, for their alleged participation in Medicare fraud schemes involving approximately $452 million in false billing.

Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, and every taxpayer who funds Medicare, is a victim.

As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used to care for the sick — not to line the pockets of criminals.

Corporate and Securities Fraud

Another area where our investigations have increased substantially in recent years is in corporate and securities fraud. Since September 2008, we have seen a 49 percent increase in these cases to more than 2,600 today.

One of our largest insider trading cases centered on the Galleon Group, a $7 billion dollar hedge fund based in New York. Using evidence obtained through court-approved wiretaps,

attorneys and corporate insiders at several Fortune 500 companies were convicted of leaking proprietary information. The owner of the Galleon Group was convicted of multiple counts of securities fraud and sentenced in October to 11 years in prison — the longest sentence ever for insider trading. And in March 2012, Allen Stanford, former chairman of the board of Stanford International Bank, was convicted on wire, mail and other fraud charges for orchestrating a $7 billion investment fraud scheme.

As financial crimes such as these become more sophisticated, so too must the FBI. In addition to devoting more agents and analysts, we established a Forensic Accountant Program three years ago. Under this program we have hired nearly 250 forensic accountants who are trained to catch financial criminals.

Three years ago, we also established the FBI's Financial Intelligence Center to strengthen our financial intelligence collection and analysis. The Center coordinates with FBI field offices to complement their resources and to identify emerging economic threats.

In 2010, the FBI began embedding Special Agents at the SEC, which allows us to see tips about securities fraud as they come into the SEC's complaint center. This, in turn, enables us to identify fraud trends more quickly and to push intelligence to our field offices so that they can begin criminal investigations where appropriate.

Gangs/Violent Crime

The most recent Uniform Crime Report (UCR) indicates violent crime continues to fall. However, for some cities and towns across the nation, violent crime – including gang activity – continues to pose a real problem.

Gangs have become more sophisticated. They have expanded their operations from street violence and drug trafficking to alien smuggling, identity theft, and mortgage fraud. Our Violent Crime, Violent Gang/Safe Streets, and Safe Trails Task Forces target major groups operating as criminal enterprises – high-level groups engaged in patterns of racketeering. This allows us to identify senior leadership and to develop enterprise-based prosecutions.

The FBI is also working to ensure crimes are being reported accurately. In collaboration with our state and local partners, the UCR program recently adopted a new, more inclusive definition of rape, which more accurately reflects current state laws defining the crime. This change will provide better data for our law enforcement partners in their efforts to respond to violent crimes. The Bureau is also beginning to look for ways to increase the accuracy and utility of the UCR more generally. These plans include collaborating within DOJ and the law enforcement community to increase the usage of the National Incident Based Reporting System (NIBRS) which is part of the UCR. Increased coverage of incident based reporting will lead to a more detailed and meaningful picture of crime in America.

Transnational Organized Crime

We also continue to confront organized crime. Crime syndicates run multi-national, multi-billion-dollar schemes – from human trafficking to health care fraud, and from computer intrusions to intellectual property theft.

These sophisticated enterprises operate both overseas and in the United States, and include Russian, Asian, Italian, Balkan, Middle Eastern, and African syndicates as well as Outlaw Motorcycle Gangs.

In the fall of 2010, an investigation by the FBI and its partners led to the indictment and arrest of more than 70 members and associates of an Armenian organized crime ring for their role in nearly $170 million in fraudulent Medicare billings. This case included more than 160 phony medical clinics. Some of the subjects opened bank accounts to receive Medicare funds and submitted applications to Medicare to become Medicare providers.

The annual cost of transnational organized crime to the U.S. economy is estimated to be in the tens of billions of dollars. The effects of these schemes filter down to everyday Americans, who pay more for gas, health care, mortgages, clothes and food, not to mention the economic and social harm that such criminal activity costs our nation as a whole.

But organized crime does more than just impact our economy. These groups have the potential to infiltrate our businesses, and provide support to hostile foreign powers.

The FBI has squads dedicated to Eurasian Organized Crime investigations, including in New York, San Francisco, Miami, Philadelphia, Newark, and Chicago. Over the past decade, Asian criminal enterprises have evolved into transnational and decentralized networks that focus on low-risk and high-profit crimes. Chinese and Korean criminal networks across the United States obtain, sell, and use fraudulent U.S. identification documents to conduct a variety of financial crimes. The FBI is currently expanding its focus to include West African and Southeast Asian organized crime groups. The Bureau continues to share intelligence about criminal groups with our federal and international partners, and to combine resources and expertise to gain a full understanding of each group. In furtherance of these efforts, the FBI participates in the International Organized Crime Intelligence Operations Center. This center is responsible for coordinating the efforts of nine federal law enforcement agencies in combating non-drug transnational organized crime networks. The FBI is also enhancing its ability to address transnational criminal enterprises that operate along the Southwest Border and the Caribbean. We have developed Hybrid Squads to target these groups, which linked to U.S.-based gangs, cross-border drug trafficking, public corruption, money laundering, and violent crime.

No one department, agency, or country can fight organized crime on its own – we must work with our partners to end this predatory environment. We will continue to use all of our investigative tools, intelligence from our sources, and the strength of our partnerships to stop organized crime in the United States.

Crimes Against Children

The FBI remains vigilant in its efforts to keep children safe and to find and stop child predators. Through our partnerships with state, local, tribal, and international law enforcement, we are able to investigate crimes that cross geographical and jurisdictional boundaries. We are also able to share intelligence, resources, and specialized skills to prevent child abductions.

Through our Child Abduction Rapid Deployment Teams, the Innocence Lost National Initiative, the 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.

Last month we added accused child pornographer Eric Justin Toth to the FBI's Ten Most Wanted Fugitive list. Toth, who also goes by the name David Bussone, is a former private-school teacher and camp counselor who taught here in Washington, D.C. He has been on the run since 2008, after an FBI investigation revealed pornographic images on a camera in his possession while at the D.C. private school. There is a reward of up to $100,000 for information leading directly to Toth's arrest.

Since its creation in 1950, the Top Ten list has been invaluable to the FBI, helping us to capture some of the nation's most dangerous criminals. Of the 495 fugitives named to the list, 465 have been apprehended or located. That level of success would not have been possible without the strong support of the public, which has helped capture 153 of the Top Ten fugitives.

Indian Country

The FBI also maintains primary federal law enforcement authority to investigate felony crimes on more than 200 Indian reservations nationwide. Last year, the FBI handled approximately 2,900 Indian Country investigations.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations concern homicide, crimes against children, or felony assaults. To address these threats, the FBI is deploying six new investigators to Indian Country as part of the Department of Justice's broader effort to fight crime in tribal communities.

The FBI continues to work with tribes through the Tribal Law & Order Act to help tribal governments better address the unique public safety challenges and disproportionately high rates of violence and victimization in tribal communities. The Act encourages the hiring of additional law enforcement officers for Indian lands, enhances tribal authority to prosecute and punish criminals, and provides the Bureau of Indian Affairs and tribal police officers with greater access to law enforcement databases.

The gang threat on Indian reservations also poses a concern for the FBI. Currently, the FBI has 15 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 tribal gaming facilities.

Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts.

We are using technology to improve the way we collect, analyze, and share information. In 2011, we debuted new technology for the FBI's Next Generation Identification System, which enables us to process fingerprint transactions much faster and with increased accuracy. We are also integrating isolated data sets throughout the Bureau, so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

Sentinel, the FBI's new information and case management program, will replace the outdated Automated Case Support System. Sentinel is transforming the way the FBI does business by moving the Bureau from a primarily paper-based case management system to an electronic workflow-based management system of records. The system's indexing ability will allow users to extract names, dates, vehicles, addresses, and other details, and to more efficiently share data with our law enforcement partners.

We expect that Sentinel will be deployed to the field by the end of this fiscal year, encompass all of its original design concept functionality and come in at budget or below.

Going Dark

As technology advances, both at the FBI and throughout the nation, we must ensure that our ability to obtain communications pursuant to court order is not eroded. The increasingly mobile, complex, and varied nature of communication has created a growing challenge to our ability to conduct court-ordered electronic surveillance of criminals and terrorists. Many communications providers are not required to build or maintain intercept capabilities in their ever-changing networks. As a result, they are too often not equipped to respond to information sought pursuant to a lawful court order.

Because of this gap between technology and the law, law enforcement is increasingly challenged in accessing the information it needs to protect public safety and the evidence it needs to bring criminals to justice. It is only by working together – within the law enforcement and intelligence communities, and with our private sector partners – that we will find a long-term solution to this growing problem. We must ensure that the laws by which we operate keep pace with new threats and new technology.

Civil Liberties/Rule of Law

Technology is one tool we use to stay one step ahead of those who would do us harm. Yet as we evolve and update our investigative techniques and use of technology to keep pace with today's complex threat environment, we always act within the confines of the rule of law and the safeguards guaranteed by the Constitution. The world around us continues to change, but our values must never change. Every FBI employee takes an oath promising to uphold the rule of law and the United States Constitution. I emphasize that it is not enough to catch the criminal; we must do so while upholding civil rights. It is not enough to stop the terrorist; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights – these are not our burdens. These are what make all of us safer and stronger. In the end, we will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

Conclusion

Chairman Leahy and Ranking Member Grassley, I thank you for this opportunity to discuss the FBI's priorities and state of the Bureau as it stands today. Mister Chairman, let me again acknowledge the leadership that you and this Committee have provided to the FBI. The transformation the FBI has achieved over the past 10 years would not have been possible without the support of Congress and the American people. I would be happy to answer any questions that you may have.