Department of Justice

STATEMENT OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

"HOMELAND THREATS AND AGENCY RESPONSES"

PRESENTED

SEPTEMBER 19, 2012

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

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

At a Hearing Entitled
"Homeland Threats and Agency Responses"

Presented
September 19, 2012

Good morning, Chairman Lieberman, Ranking Member Collins, 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 11 years ago, but today, we in the FBI are better prepared to meet that threat.

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 trade secrets and valuable research from America's companies, universities, and government agencies. Cyber threats also pose a significant risk to our nation's critical infrastructure.

As these threats continue to evolve, so too must the FBI change to counter those threats. We must continue to build partnerships with our law enforcement and private sector partners, as well as the communities we serve. Above all, we must remain firmly committed to carrying out our mission while protecting the civil rights and civil liberties of the people we serve.

Counterterrorism

Counterterrorism remains our top priority.

International Terrorism

We face a fluid, dynamic, and complex terrorist threat. We have seen an increase in the sources of terrorism, a wider array of terrorism targets, a greater cooperation among terrorist groups, and an evolution in terrorist tactics and communications methodology.

In the past decade, Al Qaeda has become decentralized, but the group remains committed to high-profile attacks against the West. Records seized from Osama bin Laden's compound more than one year ago confirm Al Qaeda's intent. The May 2012 conviction of an Al Qaeda operative who plotted to conduct coordinated suicide bombings in the New York City subway system emphasizes the reality of the threat.

Our experience has been that several key al Qaeda in the Arabian Peninsula (AQAP) figures were born or educated in the United States; they understand our culture and our security protocols, and they use this understanding to develop and refine new tactics and techniques for their proposed attacks. Al Qaeda affiliates and surrogates, especially AQAP, represent the top counterterrorism threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

AQAP leaders have published English-language articles in the Internet detailing their intent to strike the United States. They are also making use of social media to share their knowledge with individuals of similar mindsets. They realize the value of reaching English-speaking audiences, and are using the group's marketing skills to inspire individuals to undertake attacks in the United States, without having to travel or train abroad.

We also remain concerned about the threat from homegrown violent extremists. Over the past few 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 living in Boston, Massachusetts. During the fall of 2011, Ferdaus planned to use unmanned, remote-controlled aircraft to attack locations in Washington, D.C., including the U.S. Capitol. Although he espoused loyalty to Bin Laden and al Qaeda, Ferdaus was not affiliated with any group or other would-be terrorists. He had become radicalized on his own, influenced

by radical websites advocating violent extremism, among other things. In July, Ferdaus agreed to plead guilty to attempting to damage and destroy a federal building by means of an explosive and attempting to provide material support to terrorists. The agreement is subject to review and acceptance by the district court.

To better address this evolving threat, the FBI has established a Countering Violent Extremism (CVE) Office within the National Security Branch (NSB) that will 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; providing to state and local officials and to community leaders unclassified briefings regarding the threat of violent extremism; addressing CVE-related operational and mission-support needs, including investigations, analysis, and training; and coordinating the FBI's interests with regard to CVE matters with those of other agencies to ensure that the efforts of the U.S. government are aligned.

Webster Commission Report on Fort Hood

In 2009, following the attack on Fort Hood, the FBI requested a full - and independent - investigation of the manner in which the FBI handled and acted on counterterrorism intelligence before and after the Fort Hood shootings. Former FBI Director William Webster agreed to undertake that independent review. On July 19, 2012, Judge Webster delivered to the FBI the completed Webster Commission Report on Fort Hood.

The Commission found shortcomings in FBI policy guidance, technology, information review protocols, and training, and made 18 recommendations for corrective and enhancing measures in those areas. The FBI concurs with the principles underlying the recommendations and has already taken action – and had taken action, even prior to the release of the report – to implement the recommendations based on a combination of the Commission's work, the FBI's own internal review of the Fort Hood shootings, and the report of this Committee.

The Webster Commission reported that it was impressed with the quality and the commitment of the FBI's intelligence analysts and the integration of analysts into the FBI's work. The FBI has taken significant steps to strengthen the integration of intelligence and operations, and we will continue to examine innovative ways to continue our transformation from an investigative-led model to an intelligence-led model, where intelligence drives our investigative strategies, enhances our understanding of threats, and increases our ability to address and mitigate those threats. The Directorate of Intelligence will continue to evolve to more effectively provide strategic direction, oversight and support to the FBI's Intelligence Program as we expand the intelligence components in each of our operational divisions.

Domestic Terrorism

In addition to the threats related to international terrorism discussed above, we confront domestic terrorism – domestic acts of violence in furtherance of political, religious, racial, or social ideology. Unfortunately, we have seen a surge in lone offender incidents, as we witnessed with the shooting at the Sikh Temple in Wisconsin .

Many lone offenders may have some affiliation with known domestic terrorist organizations, such as violent white supremacist groups, anarchists, animal rights and environmental extremists, and militia groups, whose activities may violate federal law. These lone offenders may be loosely affiliated with such groups, but their actions typically are not directed by these groups. They may be self-trained, self-financed, and self-executing, but they are motivated to take action in furtherance of their ideological beliefs.

We in the FBI maintain comprehensive coverage of known domestic terrorist groups and their general membership. But lone offenders pose a significant concern in that they stand on the periphery.

We are working closely with our counterparts in the Department of Homeland Security to educate our law enforcement, private sector, and community partners to be on the lookout for suspicious individuals and activities. We want our partners to be attuned to the threat of domestic terrorism, whether by known groups or lone offenders, and to know how best to reach out to law enforcement for assistance.

In addition, each JTTF across the country includes Special Agents dedicated to investigating domestic terrorism. We are working with the Bureau of Prisons to combat violent radicalization of incarcerated individuals by groups with a wide range of underlying ideologies. We are also working with the Department of Defense to identify members of the military who may be affiliated with and attempt to assist or join groups engaged in terrorist activity.

In every domestic terrorism investigation – and indeed, in every investigation – we in the Bureau strive to balance our need to keep the American public safe with the constitutional rights of every citizen, including their First Amendment rights to free speech and freedom of assembly.

Cyber Security

As this Committee knows, the cyber threat has evolved and grown significantly over the past decade. Foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate government and military secrets, as well as valuable intellectual property — information that can 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. 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. And hacker groups such as Anonymous and Lulz-Sec are pioneering their own forms of digital anarchy.

With these diverse threats, we anticipate that cyber security may well become our highest priority in the years to come. Computer intrusions and network attacks are the greatest cyber threat to our national security. That is why we are strengthening our cyber capabilities, in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

We are focusing the Cyber Division on computer intrusions and network attacks. Such intrusions pose the greatest cyber threat to our national security. We will re-unite non-intrusion programs currently run by the Cyber Division, including Innocent Images and Intellectual Property Rights, with their counterparts in the Criminal Investigation Division. And because even traditional crime is now facilitated through the use of computers, we are enhancing the technological capabilities of all FBI investigative personnel. We are also hiring additional computer scientists to provide expert technical support to critical investigations in the field.

As part of these efforts, we are creating two distinct task forces in the field. First, we will have Cyber Task Forces that will be focused on intrusions and network attacks. The current cyber squads in each of our Field Offices will form the nucleus of these task forces. We must also work together to protect the most vulnerable among us: our children. To that end, we will also create Child Exploitation Task Forces in each field office, which will focus on crimes against children. As we have in the past, we welcome the participation of our federal, state and local partners, as we move forward, with these initiatives.

We are also increasing the size and scope of the National Cyber Investigative Joint Task Force – the FBI-led multi-agency focal point for coordinating and sharing of cyber threat information. The National Cyber Investigative Joint Task Force brings together 18 law enforcement, military, and intelligence agencies to stop 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.

With our partners at the Department of Homeland Security 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.

The FBI also has 63 Legal Attaché offices around the world, through which we share information and coordinate investigations with our international counterparts. We also have

Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players in the cyber arena.

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

In April 2011, 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.

And 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.

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

We must also work together to determine who is behind any given computer intrusion or network attack. 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.

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 more 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 next-generation information and case management system, was deployed to all employees on July 1, 2012. Sentinel moves the FBI from a paper-based case management system to a digital system of record. It enhances the FBI's ability to link cases with similar information through expanded search capabilities. It also streamlines administrative processes through "electronic workflow," making new case information and intelligence available more quickly to agents and analysts. The FBI will continue developing Sentinel's capabilities according to employee feedback and organizational requirements.

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 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 unable to access the information it needs to protect public safety and the evidence it need to bring criminals to justice.

We are thankful for Congress' support in funding the National Domestic Communications Assistance Center. The center will enable law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice.

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 Rights, Civil Liberties, and the Rule of Law

Intelligence and technology are key tools we use to stay ahead of those who would do us harm. Yet as we evolve and update our investigative techniques and our use of technology to keep pace with today's complex threat environment, we must 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. This oath is not to be taken lightly. In my remarks to New Agents, upon their graduation from the FBI Academy, I emphasize that it is not enough to catch the criminal; we must do so while upholding his 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 in the FBI 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 Lieberman and Ranking Member Collins, I thank you for this opportunity to discuss the FBI's priorities and the state of the Bureau as it stands today. Mr. 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 11 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.

###