STATEMENT OF ROBERT S. MUELLER, III
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE AND RELATED AGENCIES

March 19, 2013

Good morning Chairman Wolf, Ranking Member Fattah, and members of the Subcommittee. I look forward to discussing the FBI's efforts as a threat-driven, intelligence-led organization that is guided by clear operational strategies and priorities.

The FBI has established strong practices for sharing intelligence, leveraged key technologies to help us be more efficient and productive, and have hired some of the best to serve as Special Agents, Intelligence Analysts, and professional staff. We have built a workforce and leadership cadre that view change and transformation as a positive tool to keeping the FBI focused on the key threats facing our Nation.

Just as our national security and criminal adversaries and threats constantly adapt and evolve, so must the FBI be able to quickly respond with new or revised strategies and operations to counter these threats. Looking forward, a key challenge facing the FBI will be maintaining its current capabilities and capacities to respond to these threats at a time when the budgetary environment remains constrained.

We live now, and will for the foreseeable future, in a time of acute and persistent threats to our national security, economy, and community safety from terrorists, foreign adversaries, criminals and violent gangs, and cyber attackers. This Subcommittee understands these threats – and the consequences of failing to address them. I look forward to working with the Subcommittee to ensure that the FBI maintains the intelligence, investigative, and infrastructure capabilities and capacities needed to deal with these threats and crime problems within the current fiscal climate. One lesson we have learned is that those who would do harm to the Nation and its citizens will exploit any weakness they perceive in the ability and capacity of the U.S. Government to counter their activities. We must identify and fix those gaps while not allowing new weaknesses or opportunities for terrorists, cyber criminals, foreign agents, and criminals to exploit.

The threats facing the homeland, briefly outlined below, underscore the complexity and breadth of the FBI's mission to protect the nation in a post-9/11 world.

National Security Threats

Terrorism: We have pursued those who committed, or sought to commit, acts of terrorism against the United States. Along with our partners in the military and intelligence communities, we have taken the fight against terrorism to our adversaries' own sanctuaries in the far corners of the world – including Iraq, Afghanistan, Pakistan, Southwest Asia, and the Horn of

Africa. We have worked to uncover terrorist sleeper cells and supporters within the United States and disrupted terrorist financial, communications, and operational lifelines at home and abroad. We have built strong partnerships with law enforcement in countries around the world.

The threat from terrorism remains complex and ever-changing. We are seeing more groups and individuals engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication.

Threats from homegrown terrorists are also of great concern. These individuals are harder to detect, easily able to connect with other extremists, and – in some instances – highly capable operationally. There is no typical profile of a homegrown terrorist; their experiences and motivating factors are distinct.

Radicalization to violence remains an issue of great concern. No single factor explains why radicalization here at home may be more pronounced than in the past. Several factors may help frame the current dynamic. First, American extremists appear to be attracted to wars in foreign countries. We have already seen a number of Americans travel overseas to train and fight with extremist groups. The increase and availability of extremist propaganda in English perpetuates the problem.

The Internet has had a profound impact on radicalization. It has become a key platform for spreading extremist propaganda and has been used as a tool for terrorist recruiting, training, and planning. It also serves as a means of social networking for like-minded extremists.

While we have had success both in disrupting plots and obtaining convictions against numerous terrorists, we have seen an increase in the sources of terrorism, an evolution in terrorist tactics and means of communication, and a wider array of terrorist targets here at home. All of this makes our mission that much more difficult.

Foreign Intelligence. While foreign intelligence services continue traditional efforts to target political and military intelligence, counterintelligence threats now 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 poses a significant threat to national security.

Each year, foreign intelligence services and their collectors become more creative and more sophisticated in their methods to steal innovative technology, which is often the key to America's leading edge in business. Last year alone, the FBI estimates that pending economic espionage cases cost the American economy more than $13 billion. In the last four years, the number of arrests the FBI has made associated with economic espionage has doubled; indictments have increased five-fold; and convictions have risen eight-fold.

As the FBI's economic espionage caseload is growing, the percentage of cases attributed to an insider threat has increased, meaning that individuals trusted as employees and contractors are a growing part of the problem. The insider threat, of course, is not new, but it is becoming more prevalent for a host of reasons, including that theft of company information is a low-cost

route to avoid investment in research; the ease of stealing information that is stored electronically, especially when one has legitimate access to it; and the increasing exposure of businesses to foreign intelligence services as joint ventures grow and businesses becomes more global.

To address the evolving insider threat, the FBI has become more proactive to prevent losses of information and technology. The FBI continues expanding outreach and liaison alliances to government agencies, the defense industry, academic institutions, and, for the first time, to the general public, because of an increased targeting of unclassified trade secrets across all American industries and sectors.

Through these relationships, the FBI and its counterintelligence partners must continue our efforts to identify and prevent the loss of sensitive American technology.

Intelligence: Since September 11, 2001, we have improved our intelligence collection and analytical capabilities across the board. Today, we are collecting and analyzing intelligence to better understand all threats – those we know about and those that have not yet materialized. We recognize that we must always look for ways to refine our intelligence capabilities to stay ahead of these changing threats. The FBI recently restructured its Directorate of Intelligence to maximize organizational collaboration, identify and address emerging threats, and more effectively integrate intelligence and operations within the FBI. With this new structure, each office can better identify, assess, and attack emerging threats.

Cyber: As this Committee knows, the cyber arena has significantly changed over the last decade. Cyber attacks and crimes are becoming more commonplace, more sophisticated, and more dangerous. The scope and targets of these attacks and crimes encompass the full range and scope of the FBI's criminal investigative and national security missions. Traditional crime, from mortgage and health care fraud to child exploitation, has migrated online. Terrorists use the Internet to recruit, to communicate, to raise funds, to train and propagandize, and as a virtual town square, all in one. On a daily basis, we confront hacktivists, organized criminal syndicates, hostile foreign nations that seek our state secrets and our trade secrets, and for profit actors willing to hack for the right price.

Since 2002, the FBI has seen an 84 percent increase in the number of computer intrusions investigations opened. Hackers – whether state sponsored, criminal enterprises, or individuals – constantly test and probe networks, computer software, and computers to identify and exploit vulnerabilities. We are working with our partners, both foreign and domestic, to develop innovative ways to identify and confront the threat as well as mitigate the damage. There is always more work to be done, but we have had some success, including the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme.

The Rove Digital scheme infected more than four million computers located in more than 100 countries with malware. The malware secretly altered the settings on infected computers, enabling the hackers to digitally hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-routing computers to certain websites and ads. The company

received fees each time these web sites or ads were clicked on or viewed by users and generated $14 million in illegitimate income for the operators of Rove Digital.

Because Estonia has improved its domestic laws, we were able to work with our law enforcement counterparts and our private industry partners to execute a takedown of this criminal organization. Following the arrest of several co-conspirators in Estonia, teams of FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data that linked the co-conspirators to the Internet fraud scheme. At the same time, we obtained a court order in the United States to replace the rogue DNS servers with court-ordered clean servers.

In this case, we not only took down the criminal organization, but we also worked with our partners in the Department of Homeland Security (DHS) and other agencies to mitigate the damage. Seven individuals have been indicted in the Southern District of New York in this case: six in Estonia and one in Russia. The United States has sought extradition of all six Estonian subjects. To date, two of them have been remanded to U.S. custody. One pleaded guilty on February 1, 2013.

We have also worked against infrastructure we believe has been used in Distributed Denial of Service (DDOS) attacks, preventing it from being used for future attacks. Since October, the FBI and the Department of Homeland Security (DHS) have released nearly 130,000 Internet Protocol (IP) addresses determined to be infected with DDOS malware. We have released this information through Joint Intelligence Bulletins (JIBs) to 129 countries. These JIBs are released by both the DHS' Computer Emergency Readiness Team (CERT) mechanisms as well as by our Legal Attachés to our foreign partners. These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDOS attacks.

Just as the FBI has transformed its counterterrorism and intelligence programs to deal with an evolving and adapting threat, the Bureau is strengthening its cyber program and capabilities. Computer intrusions and network attacks are the greatest cyber threat to our national security. To better prioritize our cyber resources, last year we focused our Cyber Division on computer intrusions and moved all other cyber-facilitated crimes that are perpetrated over the internet to our Criminal Investigative Division. This allows the FBI to leverage resources that already exist to counter the ever-increasing cyber threat.

The FBI has also focused on hiring specialized personnel to address this growing threat. The FBI now has 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 agent of the National Cyber Investigative Joint Task Force, which includes representatives from 19 law enforcement and intelligence agency partners. The task force operates through Threat Focus Cells – smaller groups of agents, officers, and analysts focused on particular threats.

U.S. law enforcement and intelligence communities, along with our international and private sector partners, are making progress. Technological advancements and the Internet's expansion continue to provide malicious cyber actors the opportunity to harm U.S. national

security and the economy. Given the consequences of such attacks, the FBI must be able to keep pace with this rapidly developing and diverse threat.

TEDAC: The FBI established the Terrorist Explosive Devices Analytical Center, or TEDAC, in 2003. Over the past ten years, it has proved to be a valuable tool supporting the military, homeland security, international partners, intelligence, and law enforcement communities. Prior to TEDAC, no single part of our government was responsible for analyzing and exploiting intelligence related to terrorist Improvised Explosive Devices (IEDs). Today, TEDAC supports the efforts of our entire government, from law enforcement to intelligence to the military, in developing and sharing intelligence about terrorist explosive devices.

Nearly all IEDs of interest to the United States Government pass through TEDAC, allowing our technicians, examiners, scientists, and intelligence analysts to see the full spectrum of devices and to recognize trends in their construction and components. This, in turn, helps us to disarm or disrupt these devices; to link IEDs to their makers; to develop new countermeasures and most importantly, to prevent future attacks.

TEDAC has received more than 95,000 submissions since its creation. By forensically and technically exploiting IEDs and their components, scientists and engineers are able to make matches and connections between seemingly unrelated IEDs. These connections have supplied valuable information to our war fighters on the front lines, as well as law enforcement and intelligence personnel protecting the homeland. TEDAC's work has resulted in actionable intelligence and progress in the fight against increasingly sophisticated and deadly explosive devices.

Thanks to the resources provided by this committee the FBI has begun construction of a new TEDAC facility at Redstone Arsenal in Huntsville, Alabama which is expected to be complete by February 2014. This new facility will allow TEDAC operations to be collocated at a single site, allowing for more efficient and integrated forensic and intelligence activities.

Criminal Threats

The Nation faces many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent gangs and crime to public corruption. Even these threats have changed significantly since 2002. Criminal organizations – domestic and international – and individual criminal activity represent a significant threat to our security and safety in communities across the Nation. I would like to briefly highlight a number of these criminal threats – and FBI capabilities for dealing with these threats -- for the Subcommittee.

Gangs and Violent Crime: Violent crimes and gang activities exact a high toll on victimized individuals and communities. There are approximately 33,000 violent street gangs, motorcycle gangs, and prison gangs with about 1.4 million members who are criminally active in the U.S. today. A number of these gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit

their illegal activities to single jurisdictions or communities. FBI is able to work across such lines and, therefore, brings particular value to the fight against violent crime in big cities and small towns across the Nation. Every day, FBI Special Agents work in partnership with state and local officers and deputies on joint task forces and individual investigations.

FBI joint task forces – Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces – focus on identifying and targeting major groups operating as criminal enterprises. Much of the Bureau's criminal intelligence is derived from our state, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and its sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts 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: Violence and corruption associated with drug trafficking in Mexico continues to be a significant issue – not only along the Southwest Border, but in many communities throughout the U.S. where Mexican drug traffickers have established a presence. In addressing this crime problem, the FBI relies on a multi-faceted approach for collecting and sharing intelligence – an approach made possible and enhanced through the Southwest Intelligence Group, the El Paso Intelligence Center, OCDETF Fusion Center, and 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 counter violent crime and corruption that facilitates the flow of illicit drugs into the United States.

Organized Crime: Ten years ago, the image of organized crime was of hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states. That image of organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. These criminal enterprises are flat, fluid networks and have global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identify theft, trafficking of women and children, and other illegal activities. This transformation demands a concentrated effort by the FBI and federal, state, local, and international partners to prevent and combat transnational organized crime.

The FBI is expanding its focus to include West African and Southeast Asian organized crime groups. The Bureau continues to share intelligence about criminal groups with our partners, and to combine resources and expertise to gain a full understanding of each group. To further these efforts, the FBI participates in the International Organized Crime Intelligence Operations Center (IOC-2). This center serves as the primary coordinating mechanism for the efforts of nine federal law enforcement agencies in combating non-drug transnational organized crime networks.

Crimes Against Children: The 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. Investigators bring to this issue the full array of forensic tools such as DNA, trace evidence, impression evidence, and digital forensics. Through

improved communications, law enforcement also has the ability to quickly share information with partners throughout the world and our outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate both parents and children about the dangers posed by violent predators and to recover missing and endangered children should they be 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 our world a safer place for our children.

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. We have seen significant improvement in capabilities and capacities over the past decade; at the same time it is an area that remains a key concern for the future.

For example, in 2011, we deployed new technology for the FBI's Next Generation Identification System. This technology enables us to process fingerprint transactions much faster and with more accuracy. In addition, throughout the Bureau, we are also integrating isolated stand-alone data sets so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

The FBI shares information electronically with partners throughout the Intelligence Community, across the Federal government, as well as with state and local agencies. For example, the FBI works closely with the nationwide suspicious activity reporting (SAR) initiative to implement technical and business processes that enable the eGuardian system and the Information Sharing Environment's Shared Space system to share SARs more quickly and efficiently. These efforts have worked to ensure that SARs entered into Shared Space are simultaneously shared with eGuardian, and in turn, delivered to the appropriate Law Enforcement and Intelligence Community 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 and to share new case information and intelligence more quickly among Special Agents and Intelligence Analysts. It also streamlines administrative processes through "electronic workflow." The FBI will continue refining and deploying additional Sentinel features according to employee feedback and organizational requirements.

The rapid pace of advances in mobile and other communication technologies continues to present a significant challenge to conducting court-ordered electronic surveillance of criminals and terrorists. These court-ordered surveillances are often critical in cyber cases where we are

trying to identify those individuals responsible for attacks on networks, denial of services, and attempts to compromise protected information. However, there is a growing and dangerous gap between law enforcement's legal *authority* to conduct electronic surveillance, and its actual *ability* to conduct such surveillance. Because of this gap, law enforcement is increasingly unable to gain timely access to the information it needs to protect public safety and bring these criminals to justice. We are grateful for this Subcommittee's support in funding the National Domestic Communications Assistance Center, which just opened its doors last month. 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 and which provide protection to individual privacy rights keep pace with new threats and new technology.

Conclusion

Responding to this complex and ever-changing threat environment is not new to the FBI; in fact, it is now the norm. The resources this Subcommittee provides each year are critical for the FBI to be able to address existing and emerging national security and criminal threats.

Chairman Wolf, Ranking Member Fattah, and members of the Subcommittee, I would like to close by thanking you for this opportunity to discuss the FBI's priorities. Mr. Chairman, let me acknowledge the leadership that you and this Subcommittee have provided to the FBI. The transformation the FBI has achieved would not have been possible without your support. Your investments in our workforce, our technology, and our infrastructure make a difference every day at FBI offices in the United States and around the world, and we thank you for that support.

I look forward to any questions you may have.