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 7, 2012

Good morning Chairman Wolf, Ranking Member Fattah, and members of the Subcommittee. On behalf of the over 34,000 men and women of the FBI, I would like to thank you for the years of support you have provided to the Bureau.

The FBI remains focused on defending the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting civil rights and civil liberties; and providing leadership and criminal justice services to federal, state, municipal, and international agencies and partners. Our continued ability to carry out this complex and demanding mission reflects the support and oversight provided by this Subcommittee.

More than 10 years after the terrorist attacks of 9/11, the FBI continues to be a threat-focused, intelligence-driven organization that is guided by clear operational strategies. And we remain firmly committed to carrying out these strategies under guidelines established by the Attorney General that protect the civil liberties of those entrusting us with the authorities to carry out our mission.

As our Nation's national security and criminal adversaries constantly adapt and evolve, so must the FBI be able to respond with new or revised strategies and operations to counter these threats. The FBI continues to shift to be more predictive, preventative, and actively engaged with the communities we serve. The FBI's evolution has been made possible by greater use of technology to gather, analyze, and share information on current and emerging threats; expansion of collaboration with new partners, both domestically and internationally; and investments in training, developing, and maximizing our workforce. TheFBI continues to be successful in maintaining this momentum of transformation even during these challenging times.

The FBI's fiscal year (FY) 2013 budget request totals $8.2 billion in direct budget authority, including 34,083 permanent positions (13,018 Special Agents, 3,025 Intelligence Analysts, and 18,040 Professional Staff). This funding level continues increases provided to the Bureau in the past, most recently in FY 2012, allowing the FBI to maintain its forward progress, including targeting additional resources on investigating financial and mortgage fraud.

Let me briefly summarize the key national security threats and crime problems that this funding supports.

National Security Threats

Terrorism: The terrorist threat facing the United States 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.

While Osama bin Laden and certain other key leaders have been removed, al Qaeda and its affiliates and adherents continue to represent the top terrorism threat to the United States abroad and at home. Core al Qaeda remains committed to high-profile attacks against the United States. Additionally, al Qaeda affiliates and surrogates, such as al Qaeda in the Arabian Peninsula (AQAP), represent 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.

In addition to al-Qaeda and its affiliates, the United States faces a terrorist threat from self-radicalized individuals. Self-radicalized extremists – often acting on their own – are among the most difficult to detect and stop. For example, just last month, the FBI arrested Amine El Khalifi, a 29-year-old Moroccan immigrant, for the suspected attempt to detonate a bomb in a suicide attack on the U.S. Capitol Building. According to court documents, Khalifi believed he was conducting the terrorist attack on behalf of al Qaeda and had become radicalized even though he was not directly affiliated with any group. The Khalifi case exemplifies 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 basis from which acts of terrorism are committed – from organizations to affiliates/surrogates to self-radicalized individuals – continue to evolve and expand. Of particular note is al Qaeda's use of on-line chat rooms and web-sites to recruit and radicalize followers to commit acts of terrorism. And they are not hiding in the shadows of cyber space: al Qaeda in the Arabian Peninsula has produced a full-color, English-language online magazine. Terrorists are not only sharing ideas; they are soliciting information and inviting communication. Al Shabaab, the al Qaeda affiliate in Somalia, uses Twitter to taunt its enemies – in English – and encourage terrorist activity.

To date, terrorists have not used the Internet to launch a full-scale cyber attack, but we cannot underestimate their intent. Terrorists have shown interest in pursuing hacking skills. And they may seek to train their own recruits or hire outsiders, with an eye toward pursuing cyber attacks.

These adaptations of the terrorist threat make the FBI's counterterrorism mission that much more difficult and challenging.

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.

For example, last year, Noshir Gowadia was sentenced to 32 years in prison for selling secrets 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. Gowadia, a naturalized United States citizen from India, decided to offer his knowledge of sensitive design aspects of the B-2 to anyone willing to pay for it. He sold highly classified information about the B-2's stealth technology to several nations, and made six trips to China to assist them in the development of stealth technology for their cruise missiles.

Last fall, Kexue Huang, a former scientist for two of America's largest agriculture companies, pled guilty to charges that he sent trade secrets to his native 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. His criminal conduct cost Dow and Cargill millions of dollars.

And just last month, five individuals and five companies were indicted in San Francisco with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of companies controlled by the government of the People's Republic of China (PRC). According to the indictment, the Chinese government sought to obtain a proprietary chemical compound developed by DuPont to be produced in a Chinese factory.

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, U.S. government agencies, and with other components of the Department of Justice, 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: 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 national security and criminal investigative missions. Our national security secrets are regularly targeted by foreign and domestic actors; our children are targeted by sexual predators and traffickers; our citizens are targeted for fraud and identity theft; our companies are targeted for insider information; and our universities and national laboratories are targeted for their research and development. 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.

Just as the FBI has transformed its counterterrorism program to deal with an evolving and adapting threat, the Bureau is enhancing its cyber program and capabilities. To counter the cyber threat, the FBI has cyber squads in each of our 56 field offices. 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. Along with 20 law enforcement and intelligence agency partners, the FBI is the executive agent of the National Cyber Investigative Joint Task Force. The task force operates through Threat Focus Cells—smaller groups of agents, officers, and analysts from different agencies, focused on particular threats.

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.

Over the past year, the FBI and our partners have also pursued members of Anonymous, who are alleged to have coordinated and executed distributed denial of service attacks against various Internet companies. To date, 16 individuals have been arrested and charged in more than 10 states as part of this ongoing investigation. According to the indictment, the Anonymous group referred to the DDoS attacks as "Operation Avenge Assange" and allegedly conducted the attacks in support of Wikileaks founder Julian Assange. The defendants are charged with various counts of conspiracy and intentional damage to a protected computer.

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.

Criminal Threats

Criminal organizations – domestic and international – and individual criminal activity also represent a significant threat to our security and safety in communities across the Nation. The FBI focuses on many criminal threats, from white-collar crime and health care fraud to organized crime and gang violence to corruption and violence along the Southwest border. Today, I would like to highlight a number of these criminal threats for the Subcommittee.

Financial and Mortgage Fraud: From foreclosure frauds to sub-prime scams, mortgage fraud is a serious problem. The FBI continues to develop new approaches and techniques for detecting, investigating, and combating mortgage-related fraud. Through the use of joint agency task forces and working groups, the FBI and its partners work to pinpoint the most egregious offenders and identify 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 FY 2005. Nearly 70 percent of FBI's pending investigations involve losses of more than $1 million. The number of FBI Special Agents investigating mortgage fraud cases has increased from 120 in FY 2007 to 332 Special Agents in FY 2011. The multi-agency task force and working group model serves as a force-multiplier, providing an array of interagency resources and expertise to identify the source of the fraud, as well as finding the most effective way to prosecute each case, particularly in active markets where fraud is widespread.

The FBI and its law enforcement partners also 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 percent 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 FY 2013, the FBI is requesting a program increase totaling $15 million and 44 positions (40 Special Agents and 4 Forensic Accountants) to further address financial and mortgage fraud at all levels of organizations – both senior executives and lower level employees.

These resources will increase the FBI's ability to combat corporate fraud, securities and commodities fraud, and mortgage fraud, and they will enable the FBI to adapt as new fraud schemes emerge.

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, Medicaid, and other government health care programs. In 2011, the FBI had approximately 2,700 active health care fraud investigations, up approximately 7 percent 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.

The annual Health Care Fraud and Abuse Control Program report showed that the government's health care fraud prevention and enforcement efforts recovered nearly $4.1 billion in taxpayer dollars in FY 2011. This is the highest annual amount ever recovered from individuals and companies who attempted to defraud taxpayers or who sought payments to which they were not entitled.

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. The FBI also has a surge capacity that can be tapped into during major cases.

FBI joint task forces -- Violent Crime, 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 comes 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.

In addition, while the FY 2013 budget proposes to eliminate the National Gang Intelligence Center (NGIC), this will not hinder the FBI's ability to perform the analytical work done there. The FBI will continue to produce intelligence products and threat assessments, which are critical to reducing criminal gang activity in our communities. The FBI will also continue to examine the threat posed to the U.S. by criminal gangs and will focus on sharing intelligence at the field level, where intelligence sharing and coordination between DOJ agencies and state and local partners already exist. For example, our Field Intelligence Groups regularly produce intelligence products covering criminal threats, including gangs. It is through these existing resources that we will continue to produce gang-related intelligence in the absence of NGIC. In fact, the responsibility for the production of that material will happen now at the field

level where gangs operate in neighborhoods, districts and communities. The field offices are the closest to the gang problem, have a unique understanding of the gang problem and are in the best position to share that intelligence.

Violence Along the Southwest Border: The escalating violence associated with drug trafficking in Mexico continues to be a significant issue. 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. The FBI is also cooperating closely with the government of Mexico in their efforts to break the power of the drug cartels inside the country.

Most recently, the collective efforts of the FBI, the Drug Enforcement Administration and other U.S. and Mexican law enforcement partners resulted in the identification and indictment of 35 leaders, members, and associates of one of the most brutal gangs operating along the U.S.-Mexico border on charges of racketeering, murder, drug offenses, money laundering, and obstruction of justice. Of these 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.

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.

For example, late last year, an investigation by the FBI and its partners led to the indictment and arrest of over 70 members and associates of an Armenian organized crime ring for their role in nearly $170 million in health care fraud. 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.

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. 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 globalization, 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.

Offsets

The FBI's FY 2013 budget request proposes offsets totaling approximately $63 million, including program reductions. Proposed offsets, which are expected to result in little if any impact on the missions and responsibilities of the FBI, include: elimination of the National Gang Intelligence Center; reduction of one training day and equipment provided for federal, state and local bomb technicians and the Special Weapons and Tactics (SWAT) and Hostage Rescue Team (HRT) training; reduction of contractor workforce funding supporting national security programs; reductions in funding for permanent change of station transfers, which relocates staff to meet organizational needs and carry out mission requirements; and reducing funding for information technology, facilities, and other administrative initiatives. We will work to sustain our efforts in these program areas and minimize the impact of these proposed reductions.

Conclusion

Responding to this complex and ever-changing threat environment is not new to the FBI; in fact, it is now the norm. The budget proposed for the FBI for FY 2013 seeks to maintain current capabilities and capacities achieved through increases provided in the past, as well as target additional resources to address financial and mortgage fraud. These resources 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 again thanking you for this opportunity to discuss the FBI's priorities and detail the FBI's FY 2013 Budget request. Mr. Chairman, let me again acknowledge the leadership that you and this Subcommittee have provided to the FBI. The transformation the FBI has achieved over the past ten years 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.