

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

April 7, 2011

Good morning Chairwoman Mikulski, Ranking Member Hutchison, and members of the Subcommittee.

On behalf of the over 30,000 men and women of the FBI, I would like to thank you for the years of support you have provided to the Bureau. This Subcommittee has been instrumental in ensuring the FBI has received the critical resources it needs to: defend the United States against terrorism and foreign intelligence threats; uphold and enforce the criminal laws of the United States; protect civil rights and civil liberties; and provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

Since 9/11, the FBI has shifted to be an intelligence-led, threat-focused organization, guided by clear operational strategies. The FBI is focused on predicting and preventing the threats we face, while engaging the communities we serve. This shift has led to a greater reliance on technology, collaboration with new partners, and human capital, requiring additional resources. The FBI is a full member of the U.S. intelligence community and serves as a critical and singular link between the intelligence and law enforcement communities in the United States. The FBI, as an organization, is in a unique and critical position to address national security and criminal threats that are increasingly intertwined. Our adversaries are evolving and using globalization to enhance their reach and effectiveness, creating new challenges in our efforts to counter their impact.

Today, the diversity and complexity of the threats facing the homeland has never been greater:

- In the past year, the United States has been the target of terrorist plots from three main sources: al Qaeda, al Qaeda's affiliates, and homegrown extremists. Homegrown extremists are a growing concern and priority of the FBI, as evidenced by the number of recent disruptions and arrests.
- The asymmetric intelligence threat presented by certain foreign governments endures as the damage from compromised sensitive information and financial losses from economic espionage and criminal activity remain significant.

- Technological advancements and the Internet's expansion will continue to empower malicious cyber actors to harm U.S. national security through criminal and intelligence activities. We must maintain our ability to keep pace with this rapidly developing technology.
- The FBI's efforts prosecuting financial crimes—including billion-dollar corporate and mortgage frauds, massive Ponzi schemes, and sophisticated insider trading activities—remain essential to protect investors and the financial system, as well as homeowners and ultimately taxpayers. There also continue to be insidious health care scams that endanger patients and fleece government health care programs of billions. Despite strong enforcement, both public corruption and violent gang crimes continue to endanger our communities.

These examples underscore the complexity and breadth of the FBI's mission to protect the nation in a post-9/11 world.

The FBI's FY 2012 Budget request includes a total of \$8.1 billion in direct budget authority, including 33,469 permanent positions (12,993 Special Agents, 2,989 Intelligence Analysts, and 17,487 Professional Staff). This funding, which consists of \$8.0 billion in Salaries and Expenses and \$81.0 million in Construction, is critical to continue our progress acquiring the intelligence and investigative capabilities required to counter current and emerging national security and criminal threats.

Consistent with the Bureau's transformation to a threat-informed and intelligence-driven agency, the FY 2012 Budget request was formulated based upon our understanding of the major national security and criminal threats that the FBI must work to prevent, disrupt, and deter. We then identified the gaps and areas which required additional resources. As a result of this integrated process, the FY 2012 budget proposes \$131.5 million for new or expanded initiatives and 181 new positions, including 81 Special Agents, 3 Intelligence Analysts, and 97 Professional Staff. These additional resources will allow the FBI to improve its capacity to address threats in the priority areas of terrorism, computer intrusions, weapons of mass destruction, foreign counterintelligence, and violent crime.

Let me briefly summarize the key national security threats and crime problems that this funding enables the FBI to address.

National Security Threats

Terrorism: The FBI is fully engaged in the worldwide effort to counter terrorism. We have taken that fight to our adversaries' own sanctuaries in the far corners of the world – Iraq, Afghanistan, Pakistan, Europe, Asia, and Africa. We have also worked to uncover terror cells and supporters within the United States, as well as disrupting terrorists' financial, communications, and operational lifelines at home and abroad.

Al Qaeda remains our primary concern. Al Qaeda's intent to conduct high-profile attacks inside the United States is unwavering. While the overall structure of the group has diminished, its power to influence individuals and affiliates around the world has not. Today, we still confront the prospect of a large-scale attack by Al Qaeda, but the growing threat from Al Qaeda affiliates, as demonstrated in the attempted Christmas Day bombing and the failed Times Square bombing, is unprecedented. Al Qaeda and its affiliates may also attempt smaller attacks that require less planning and fewer operational steps – attacks that may be more difficult to detect and prevent.

Threats from homegrown terrorists are also of growing 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 vary widely.

The added problem of radicalization makes these threats more dangerous. No single factor explains why radicalization here at home may be more pronounced than in the past. American extremists appear to be attracted to wars in foreign countries, as we have seen a number of Americans travel overseas to train and fight with extremist groups. These individuals may be increasingly disenchanted with living in the United States, or angry about U.S. and Western foreign policy. The increase and availability of extremist propaganda in English can exacerbate the problem.

The Internet has also become a key platform for spreading extremist propaganda and has been used as a tool for terrorist recruiting, training, and planning, and has been used as a means of social networking for like-minded extremists. Ten years ago, in the absence of the Internet, extremists would have operated in relative isolation, unlike today.

In short, 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 and requires continued support.

The FY 2012 Budget request includes 63 positions (34 Special Agents) and \$40.9 million to address these national security threats, including funding for surveillance resources to combat International Terrorism and foreign intelligence threats, as well as funding for the High-Value Detainee Interrogation Group (HIG), Terrorist Screening Center operations, and increased information analysis and sharing capabilities.

Intelligence: Since 9/11, the FBI has dramatically shifted our intelligence program and capabilities to address emerging threats. We stood up the National Security Branch, created a Directorate of Intelligence, integrated our intelligence program with other agencies in the Intelligence Community, hired hundreds of Intelligence Analysts and Linguists, and created Field Intelligence Groups in each of our 56 Field Offices. In short, the FBI improved and expanded our intelligence collection and analytical capabilities across the board.

Today, we are collecting intelligence to better understand all threats – those we know about and those that have not yet materialized. We recognize that we must continue to refine our intelligence capabilities to stay ahead of these changing threats. We must function as a threat-driven, intelligence-led organization. The FBI recently restructured its Field Intelligence Groups, where each group now has clearly defined requirements for intelligence collection, use, and production. With this new structure, each office can better identify, assess, and attack emerging threats.

We want to make sure that every agent in every field office approaches a given threat in the same manner, and can better turn information and intelligence into knowledge and action. The FY 2012 Budget request includes \$2.5 million to help with this endeavor.

Cyber: A cyber attack could have a similar impact as a well-placed bomb. To date, terrorists have not used the Internet to launch a full-scale cyber attack, but they have executed numerous denial-of-service attacks and defaced numerous websites.

Al Qaeda's online presence has become almost as potent as its physical presence. Extremists are not limiting their use of the Internet to recruitment or radicalization; they are using it to incite terrorism. Of course, the Internet is not only used to plan and execute attacks; it is also a target itself. Osama bin Laden long ago identified cyberspace as a means to damage both our economy and our morale – and countless extremists have taken this to heart.

The FBI, with our partners in the Intelligence Community, believe the cyber terrorism threat is real and is rapidly expanding. Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward coupling physical attacks with cyber attacks.

The FBI pursues cyber threats from start to finish. We have cyber squads in each of our 56 Field Offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners. Together, they run complex undercover operations and examine digital evidence. They share information with our law enforcement and intelligence partners. And they teach their counterparts—both at home and abroad—how best to investigate cyber threats.

But the FBI cannot do it alone. The National Cyber Investigative Joint Task Force includes 18 law enforcement and intelligence agencies, working side by side to identify key players and schemes. This task force plays an important role in the Administration's Comprehensive National Cybersecurity Initiative. Its goal is to predict and prevent that which is on the horizon, and then attribute and pursue the enterprises behind these attacks. The task force operates through Threat Focus Cells—smaller groups of agents, officers, and analysts from different agencies, focused on particular threats.

Together, with law enforcement, the Intelligence Community, and our international and private sector partners, we are making progress, but there is

significantly more to do. The FY 2012 Budget request includes 42 positions (14 Special Agents) and \$18.6 million to enhance the FBI's investigatory capabilities and protect critical technology network infrastructure from malicious cyber intrusions as well as improve analysis of digital evidence.

Technology and Tools: The FBI has greatly improved the way we collect, analyze, and share information using technology. Intelligence provides the information we need, but technology further enables us to find the patterns and connections in that intelligence. Through sophisticated, searchable databases, we are working to track down known and suspected terrorists through biographical and biometric information, travel histories and financial records. We then share that information with those who need it, when they need it.

For example, the FBI has developed the Data Integration and Visualization System (DIVS), with the goal to prioritize and integrate disparate datasets across the Bureau. The FBI currently has investigative data that is stored and accessed in multiple systems. As a consequence, our personnel are spending too much time hunting for data, leaving them less time to analyze and share that data to stay ahead of threats. Furthermore, this stove-piped architecture and inefficient process increases enterprise costs and impedes the speed, effectiveness, and responsiveness of intelligence and investigative analysis.

DIVS provides single sign-on, role-based access controls to analyze and link all FBI data that the user is lawfully allowed to see and will provide the means to efficiently feed FBI Secret data to the FBI Top Secret system. DIVS will not only significantly improve users' efficiency in searching multiple databases, it will ultimately help reduce or eliminate unnecessarily redundant data systems.

In addition to creating new technologies, like DIVS, one lesson we have learned in recent years is the need to ensure that as new technology is introduced into the marketplace, the FBI and its law enforcement partners maintain the technical capabilities to keep pace. In the ever-changing world of modern communications technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications.

As the gap between authority and capability widens, the Federal government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage – evidence that a court has authorized us to collect. We need to ensure that our capability to execute lawful court orders to intercept communications does not diminish as the volume and complexity of communications technologies expand.

The FBI's FY 2012 Budget request includes 23 positions (3 Special Agents) and \$20.5 million to advance DIVS development and to strengthen the FBI's and our law enforcement partners' ability to successfully conduct lawfully-authorized electronic

surveillance, consistent with existing authorities, by establishing a Domestic Communications Assistance Center (DCAC).

Weapons of Mass Destruction: The FBI carries responsibility for responding to certain Weapons of Mass Destruction (WMD) threats in the United States, and the WMD Directorate carries out that critical charge. The Directorate was established to be a unique combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise that exists nowhere else in the U.S. government. The creation of the Directorate enabled the FBI to focus its WMD preparedness, prevention, and response capabilities in a single, focused organization rather than through decentralized responsibilities across divisions.

The global WMD threat to the United States and its interests continues to be a serious concern. The WMD Commission has warned that without greater urgency and decisive action, it is more likely than not that a WMD will be used in a terrorist attack somewhere in the world by the end of 2013. Osama bin Laden has also said that obtaining a WMD is a “religious duty” and is reported to have sought to perpetrate a “Hiroshima” on U.S. soil.

Globalization makes it easier for terrorists, other groups, and lone actors to gain access to and transfer WMD materials, knowledge, and technology throughout the world. As noted in the WMD Commission’s report, those intent on using WMDs have been active and as such “the margin of safety is shrinking, not growing.”

The frequency of high-profile acts of terrorism has increased over the past decade. Indicators of this increasing threat include the 9/11 attacks, the 2001 Amerithrax letters, the possession of WMD-related materials by Aafia Siddiqui when she was captured in 2008, and multiple attempts by terrorists at home and abroad to use explosives improvised from basic chemical precursors. The challenge presented by these threats is compounded by the large volume of hoax threats that distract and divert law enforcement agencies from addressing real threats.

The FBI must be poised to handle any WMD event, hoax or real. Therefore, the FY 2012 Budget request includes 13 positions (including 6 Special Agent Bomb Technicians) and \$40.0 million to acquire the necessary aircraft required to respond to a WMD incident and render a device safe.

Criminal Threats

The FBI faces many criminal threats, from white collar crime to Organized Crime to violent crime and gangs to the extreme violence along the Southwest Border. While all of these threats remain, I would like to take the opportunity to focus on two of these threats – investigations along the Southwest border and violent crime occurring in Indian Country (IC).

Southwest Border: The U.S. border with Mexico extends nearly 2,000 miles, from San Diego, California to Brownsville, Texas. At too many points along the way, drug cartels transport kilos of cocaine and marijuana, gangs kidnap and murder innocent civilians, traffickers smuggle human cargo, and corrupt public officials line their pockets by looking the other way. Any one of these offenses represents a challenge to law enforcement. Taken together, they constitute a threat not only to the safety of our border communities, but to the security of the entire country.

The severity of this problem is highlighted by the following statistics:

- \$18 - \$39 billion flow annually from the U.S. across the Southwest Border to enrich the Mexican drug cartels.
- 2,600 drug-related murders in Juarez, Mexico in 2009.
- 28,000 drug-related murders in all of Mexico since 2006.
- 93 percent of all South American cocaine moves through Mexico on its way to the United States.
- 701,000 kilograms of marijuana seized during the first five months of 2010 in Southwest Border states (Arizona, California, New Mexico, and Texas).
- 6,154 individual seizures of marijuana, cocaine, heroin, and methamphetamines during the first five months of 2010 in the Southwest Border states.

The FBI has 13 border corruption task forces, but to address security along the Southwest Border, we have developed an intelligence-led, cross-programmatic strategy to penetrate, disrupt and dismantle the most dangerous organizations and individuals. This strategy begins with the deployment of hybrid squads in hotspot locations. The primary goal of the hybrid squad model is to bring expertise from multiple criminal programs into these dynamic, multi-faceted threats and then target, disrupt, and dismantle these organizations. Hybrid squads consist of multi-disciplinary teams of Special Agents, Intelligence Analysts, Staff Operations Specialists, and other professionals. The agent composition on the squads provides different backgrounds and functional expertise, ranging from violent gangs, public corruption, and violent crimes.

The FBI's FY 2012 Budget request includes funding to continue these efforts, which were initially provided through Supplemental funding in FY 2010.

Indian Country: The FBI has the primary federal law enforcement authority for felony crimes in Indian Country. Even with demands from other threats, Indian Country law enforcement remains a priority for the FBI. Last year, the FBI was handling more than 2,400 Indian Country investigations on approximately 200 reservations and over 400 Indian gaming facilities throughout 28 states. Approximately 75 percent of all FBI Indian Country investigations involve homicide, crimes against children, or felony assaults. American Indians and Alaska Natives experience violent crime at far higher rates than other Americans. Violence against Native women and children is a particular

problem, with some counties facing murder rates against Native women well over 10 times the national average.^[1]”

Complex jurisdictional issues and the dynamic and growing threat in Indian Country requires additional FBI presence. Currently, the FBI has 18 Safe Trails Task Forces focused on drugs, gangs and violent crimes in Indian Country. The gang threat on Indian Reservations has become evident to the tribal community leaders, and gang related violent crime is reported to be increasing. Tribal communities have reported that tribal members are bringing back gang ideology from major cities, and Drug Trafficking Organizations are recruiting tribal members.

In order to address this situation, the FBI’s FY 2012 Budget request includes 40 positions (24 Special Agents) and \$9.0 million to bolster existing Safe Trails Task Forces and to provide additional investigative resources to address a significant Violent Crime threat in Indian Country.

Offsets

The FBI, like all federal organizations, must do its part to create efficiencies. Although the FBI’s FY 2012 Budget request includes \$131.5 million in program increases, it is offset, in part, by almost \$70 million in program reductions. These offsets include \$26.3 million to reduce funding for the FBI’s Secure Work Environment program, which enables the FBI’s national security workforce the ability to access and Top Secret information within the FBI and with Intelligence Community partners; almost \$1 million to eliminate and consolidate FBI Violent Crime and Gang Task Forces; a \$15 million reduction to Sentinel (the FBI’s case management system); \$6.3 million to reduce support of the relocation program, which strategically relocates staff to meet organizational needs and carry out mission requirements; almost \$1 million to eliminate 12 FBI Resident Agency offices across the country; a \$5.8 million reduction to the FBI’s ability to develop new tools to identify and analyze network intrusions; a \$2.6 million reduction as a result of surveillance program efficiencies; almost \$1 million to reduce the amount requested to hire and support Special Agents and Intelligence Analysts; \$5.7 million to delay the refreshment cycle of FBI desktop and laptop computers – delaying refreshment from four years to five or more years; and a \$5.9 million reduction for administrative efficiencies, including funding for travel, equipment, conferences and office supplies.

Conclusion

Chairwoman Mikulski, Ranking Member Hutchison, and Members of the Subcommittee, I want to thank you for this opportunity to discuss the FBI’s priorities and detail new investments sought for FY 2012. Madam Chairwoman, let me again acknowledge the leadership and support that you and this Committee have provided to

^[1] Zaykowski, Kallmyer, Poteyeva, & Lanier (Aug. 2008), *Violence Against American Indian and Alaska Native Women and the Criminal Justice Response: What is Known*, Bachman (NCJ # 223691), at 5, <http://www.ncjrs.gov/pdffiles1/nij/grants/223691.pdf>.

the FBI. Congress' funding of critical investments in people and technology are making 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.