Department of Justice

STATEMENT OF
ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"SECURING AMERICA'S SAFETY: IMPROVING THE EFFECTIVENESS OF ANTI-TERRORISM TOOLS AND INTER-AGENCY COMMUNICATION"

PRESENTED
JANUARY 20, 2010

Robert S. Mueller, III
Director
Federal Bureau of Investigation
before the
Committee on the Judiciary
United States Senate
January 20, 2010

"Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication"

I. Introduction

Good morning Chairman Leahy, Senator Sessions, and members of the Committee. I am pleased to be here today.

As you know, we in the FBI have undergone unprecedented transformation in recent years, from developing the intelligence capabilities necessary to address emerging terrorist and criminal threats, to creating the administrative and technological structure to meet our mission as a national security service.

We have worked to become a full partner in the Intelligence Community. With that comes the responsibility to ensure that we consistently collect, analyze, and disseminate intelligence to those who need it, from our Federal partners in the Central Intelligence Agency (CIA), the National Counterterrorism Center (NCTC), the Office of the Director of National Intelligence (ODNI), and the Department of Homeland Security (DHS), among others, to our international, State, local, and tribal counterparts. As I have often said, today we share information by rule, and withhold by exception.

As recent events indicate, terrorists remain determined to strike the United States. We are particularly concerned about individuals who may be radicalized overseas, both those who live in America and those who live overseas and who may one day return to the United States to

perpetrate terrorist attacks. We in the FBI, with our partners in the Intelligence Community, must do everything possible to ensure that does not happen. This will require constant vigilance on the FBI's part, and on the part of every member of the IC. It will require the best and highest use of the intelligence we collect, both individually and as a group.

II. The Changing Terrorist Threat

I want to focus first on the changing terrorist threat.

As the Christmas Day attempted bombing illustrates, the threats we face are becoming more diverse and more dangerous with each passing day. We not only face threats from Al Qaeda, but also from self-directed groups not part of Al Qaeda's formal structure which have ties to terrorist organizations through money or training.

We face threats from homegrown terrorists – those who live in the communities they intend to attack, and who are self-radicalizing, self-training, and self-executing. We face threats from those who may attend training camps overseas – individuals who may live here in the United States, and who may be radicalized here or overseas, and those who may live overseas but plan to travel to the United States to perpetrate attacks.

We also face threats from extremists operating in new sanctuaries around the world. While we disabled Al Qaeda's training and financing mechanisms in Afghanistan in the wake of the September 11th attacks, it is clear that Al Qaeda and its offshoots are rebuilding in Pakistan, Yemen, and the Horn of Africa.

At the same time, we cannot discount the lone offender threat here at home – the individual who may take up arms and strike without notice.

We are using intelligence to identify these potential threats. But the question remains: How do we take the strategic intelligence we possess and turn it into tactical intelligence? In other words, once we have identified a potential threat, how do we determine who might take action, and where and when they may do so? And more importantly, how do we prevent them from doing so?

In recent years, our capacity for intelligence analysis has improved dramatically. But as the saying goes, trying to glean actionable intelligence from the flood of information we receive is akin to taking a sip of water from a fire hose. As I noted above, the challenge for all members of the IC is to find links between disparate pieces of information – to use the intelligence we possess, individually and collectively – to form a clear picture about the intentions of our adversaries.

III. Recent Counterterrorism Disruptions

As illustrated by recent events, the terrorist threat has not diminished. But through enhanced intelligence, improved technology, and strong partnerships, we have been able to disrupt several terrorist threats and plots this year.

For example, on December 14, 2009, in Georgia, Ehsanul Islam Sadequee was sentenced to 17 years in prison on charges of material support to terrorists. Syed Harris Ahmed was sentenced to 13 years on similar charges. These individuals conducted surveillance of potential targets in Washington, D.C., and pursued terrorist training overseas. They were part of an online network that connected extremists in North America, Europe, and South Asia.

This past October, in Chicago, U.S. citizen David Headley was arrested for planning terrorist attacks against a Danish newspaper and two of its employees. Headley is alleged to have conducted extensive surveillance of targets in Mumbai for more than two years preceding the November 2008 attack there. Headley is also alleged to have attended terrorist training camps in Pakistan. On January 14, 2010, a superseding indictment was filed against Headley relating to his conspiring with others to plan and execute attacks in both Denmark and India.

In October 2009, in Massachusetts, members of the FBI's Joint Terrorism Task Force arrested Tarek Mehanna on charges of conspiracy to provide material support to terrorists. Federal officials charge that Mehanna and other conspirators discussed their desire to participate in violent jihad against America, including a plot to use automatic weapons to open fire on shoppers and emergency responders at shopping malls in Boston.

In Minnesota, 14 individuals have been charged in recent months as part of an ongoing investigation into the recruitment of persons from U.S. communities to train with or fight on behalf of extremist groups in Somalia. Four defendants have pled guilty and await sentencing. Charges include providing financial support to those who traveled to Somalia to fight on behalf of al Shabaab, attending terrorist training camps operated by al Shabaab, and fighting on behalf of al Shabaab.

In September 2009, Colorado resident Najibullah Zazi was arrested in New York and was charged with conspiracy to use weapons of mass destruction (explosives) in the United States. As alleged in the indictment, Zazi had received detailed bomb-making instructions in Pakistan. Zazi allegedly purchased components of improvised explosive devices, and had traveled to New York City on September 10, 2009, in furtherance of his criminal plans.

Also in September of last year, in Illinois, FBI Special Agents arrested Michael C. Finton on charges of attempted murder of Federal employees and attempted use of a weapon of mass destruction (explosives) in connection with a plot to detonate a vehicle bomb at a Federal building in Springfield. In his efforts to carry out the plot, Finton communicated with undercover FBI agents and confidential sources that continuously monitored his activities up to the time of his arrest. According to the complaint, Finton also drove a vehicle containing inactive explosives to the Federal courthouse in Springfield and attempted to detonate them.

That same month, in Texas, Hosam Smadi was charged with attempting to use a weapon of mass destruction. Smadi, who was under continuous surveillance by the FBI, was arrested after he placed an inert car bomb near a 60-story office tower in downtown Dallas. As alleged in the indictment, Smadi, a Jordanian citizen in the United States illegally, has repeatedly espoused his desire to commit violent jihad and had been the focus of an undercover FBI investigation.

This past July, in North Carolina, FBI agents arrested an alleged group of homegrown terrorists who were heavily armed and making plans to wage jihad overseas. The seven men arrested – including a father and his two sons – were charged with providing material support to terrorists and conspiring to murder, kidnap, and injure people overseas. The father, Daniel

Patrick Boyd, once fought in Afghanistan, and allegedly trained in terrorist camps in Pakistan and Afghanistan. All of the defendants but one are U.S. citizens.

And last May, in New York, four individuals were arrested on charges of conspiracy to use weapons of mass destruction in the United States and conspiracy to acquire and use anti-aircraft missiles. The group allegedly plotted to blow up a Jewish synagogue in the Bronx and to shoot down military planes at the New York Air National Guard Base. As alleged in the indictment, they obtained what they believed to be three improvised explosive devices and a Stinger surface-to-air guided missile from a source who was in fact an FBI informant.

This is merely a sampling of the investigations we have handled over the past year. In each investigation, the resources and the investigative experience of our Federal, State, and local law enforcement and intelligence counterparts proved invaluable. Indeed, we in the FBI could not do our jobs without their critical assistance and their expertise.

IV. December 25, 2009 Attack

On January 6, 2010, Umar Farouk Abdulmutallab, a 23-year-old Nigerian national, was charged in a six-count criminal indictment for his alleged role in the attempted Christmas day bombing of Northwest Airlines flight 253 from Amsterdam, the Netherlands, to Detroit.

Abdulmutallab has been charged with attempted use of a weapon of mass destruction, attempted murder within the special aircraft jurisdiction of the United States, willful attempt to destroy an aircraft, willfully placing a destructive device on an aircraft, use of a firearm or destructive device during and in relation to a crime of violence, and possession of a firearm or destructive device in furtherance of a crime of violence.

According to the indictment, Northwest Airlines flight 253 carried 279 passengers and 11 crew members. Abdulmutallab allegedly boarded Northwest Airlines flight 253 in Amsterdam on December 24, 2009, carrying a concealed bomb. The bomb components included Pentaerythritol (also known as PETN, a high explosive) and Triacetone Triperoxide (also known as TATP, a high explosive), and other ingredients.

The bomb was concealed in the defendant's underclothing and was designed to allow him to detonate it at a time of his choosing, thereby causing an explosion aboard flight 253, according to the indictment. Shortly prior to landing at Detroit Metropolitan Airport, on December 25, 2009, Abdulmutallab allegedly detonated the bomb, causing a fire on board the plane.

According to an affidavit filed in support of the criminal complaint, Abdulmutallab was subdued and restrained by passengers and the flight crew after allegedly detonating the bomb. The airplane landed shortly thereafter, whereupon U.S. Customs and Border Protection officers took him into custody.

The FBI is responsible for investigating this incident. FBI Special Agents interviewed Abdulmutallab following the attack, and have shared all relevant information with our partners in the IC. We will continue to investigate Abdulmutallab and all individuals connected to him, and we will continue to share all relevant information with our law enforcement and intelligence counterparts. However, because this is an ongoing investigation, we cannot divulge many details at this juncture.

V. Terrorist Watchlisting Procedures

I would like to turn for a moment to terrorist watchlisting procedures and the Terrorist Screening Center ("TSC")

The TSC is a multi-agency center that connects the law enforcement communities with the IC by consolidating information about known and suspected terrorists into a single Terrorist Watchlist. The TSC facilitates terrorist screening operations, helps coordinate the law enforcement responses to terrorist encounters developed during the screening process, and captures intelligence information resulting from screening.

The TSC integrates the law enforcement and intelligence communities by consolidating terrorist information. The current terrorist watchlisting and screening enterprise is a collaborative effort between the TSC, the FBI, DHS, the Department of State, the Department of Defense, the NCTC, and other members of the IC.

VI. Today's FBI

A. Restructuring of FBI Intelligence Program

To meet our national security mission, we have expanded our counterterrorism operations and honed our intelligence capabilities. We stood up the National Security Branch and the Weapons of Mass Destruction Directorate. We integrated our intelligence program with other agencies under the Director of National Intelligence, with appropriate protections for privacy and civil liberties. We hired hundreds of intelligence analysts, linguists, and surveillance specialists. And we created Field Intelligence Groups in each of our 56 field offices. In short, we improved our national security capabilities across the board.

But we also recognize that we must continue to move forward, to refine programs and policies already in place, and to make necessary changes to our intelligence program.

To that end, we established a Strategic Execution Team, or SET, to help us assess our intelligence program, and to standardize it throughout the Bureau. The SET, made up of agents and analysts, developed a series of recommendations for accelerating the integration of our intelligence and investigative work.

The SET improvements ensure that we capitalize on our intelligence collection capabilities and develop a national collection plan to fill gaps in our knowledge base. Our objective is to defeat national security and criminal threats by operating as a single intelligence-led operation, with no dividing line between our criminal and counterterrorism programs. In short, we want to make sure that nothing falls through the cracks.

To this end, we have restructured the Field Intelligence Groups, or FIGs, in every field office across the country. FIGs are designed to function as the hub of the FBI's intelligence program. They ensure that each field office is able to identify, assess, and attack emerging threats before they flourish.

Following the SET's recommendations, the FIGs now conform to one model, based on best practices from the field, and adapted to the size and complexity of each office. Each FIG

has well-defined requirements for intelligence gathering, analysis, use, and production. And managers are accountable for ensuring that intelligence production is of high quality and relevant not only to their own communities, but to the larger intelligence and law enforcement communities.

As a result of these changes, the FIGs can better coordinate with each other and with Headquarters. They can better coordinate with law enforcement and intelligence partners, and the communities they serve. With this integrated model, we can turn information and intelligence into knowledge and action, from coast to coast.

These changes are part and parcel of our ongoing campaign to "Know Our Domain," as we say. Domain awareness is a 360-degree understanding of all national security and criminal threats in any given city, community, or region. It is the aggregation of intelligence, to include what we already know and what we need to know, and the development of collection plans to find the best means to answer the unknowns. With this knowledge, we can identify emerging threats, allocate resources effectively, and identify new opportunities for intelligence collection and criminal prosecution.

We have implemented SET concepts at FBI Headquarters, to improve strategic alignment between the operational divisions and the Directorate of Intelligence. We want to better manage national collection requirements and plans, and ensure that intelligence from our Field Offices is integrated and shared with those who need it at FBI Headquarters and in the larger Intelligence Community.

We will continue to refine not only the manner in which we collect and share information, but the manner in which we analyze that information, to find links between people, cases, and countries.

B. Improvements to FBI Technology

We have also made a number of improvements to the FBI's information technology systems. We cannot gather the intelligence we need, analyze that intelligence, or share it with our law enforcement or intelligence partners, without the right technology.

As you know, we continue to implement Sentinel, our web-based case management system, which makes it faster and easier to access and connect information from office to office, from case to case, and from program to program.

We are also strengthening the IT programs that allow us to communicate and share with our partners. For example, we are consolidating the FBI's Unclassified Network with Law Enforcement Online, or LEO, which is the unclassified secure network we use to share information with registered law enforcement partners. This will provide a single platform that allows FBI employees to communicate and share with their internal and external partners. Currently, LEO provides a secure communications link to all levels of law enforcement and is available to more than 18,000 law enforcement agencies.

As part of the LEO platform, the FBI is delivering the eGuardian system – an unclassified counterterrorism tool available to our Federal, State, local, and tribal law enforcement partners through the FBI's secure LEO internet portal. eGuardian makes threat and suspicious activity information immediately available to all authorized users. The eGuardian system will work in tandem with Guardian, enabling law enforcement personnel to receive the most current information. In return, any potential terrorist threat or suspicious activity information provided by law enforcement will be made available in Guardian entries and pushed outward to the FBI task forces.

We are also in the midst of developing what we call "Next Generation Identification" system, which expands the FBI's fingerprint-based identification, known as IAFIS, to include additional biometric data. This will better enable us to find criminals and terrorists who are using the latest technology to shield their identities and activities.

We are also working to improve our confidential human source management system. Intelligence provided by confidential human sources is fundamental to the FBI mission. To better manage that data, we have implemented a program known as DELTA. DELTA will provide FBI agents and intelligence analysts a uniform means of handling the administrative aspect of maintaining human sources. It will also enable FBI Headquarters and Field Offices to better understand, connect, operate, and protect confidential human sources.

Finally, we are improving our crisis management systems. The Operational Response and Investigative Online Network (ORION) is the FBI's next-generation Crisis Information Management System. ORION provides crisis management services to Federal, State, local, and tribal law enforcement and/or emergency personnel. It standardizes crisis and event management processes, enhances situational awareness, and supports the exchange of information with other command posts.

The ORION application is accessible from almost any desktop with FBINET or UNET connectivity using a standard web browser, or by other secure connections providing access to Federal, State and local law enforcement partners It has been used at both the Democratic and Republican national conventions, major sporting events, to include the Olympics, and last year's Presidential Inauguration.

These improvements are necessary for the work ahead of us, and we will continue to develop and implement the necessary tools to combat today's diverse, dangerous, and global threats together with our partners in the law enforcement and intelligence communities.

VII. Conclusion

Over the past 100 years, the FBI has earned a reputation for protecting America that remains unmatched. Many of our accomplishments over the past eight years are in part due to your efforts and your support, and much of our success in the years to come will be due to your continuing support. From protecting the American people from terrorist attack to addressing the growing gang problem to creating additional Legal Attaché offices around the world, you have supported our mission and our budget requests.

Mr. Chairman, I would like to conclude by thanking you and this Committee for your service and your support. On behalf of the men and women of the FBI, I look forward to working with you in the years to come. I would be happy to answer any questions you may have.

# # #