Department of Justice

STATEMENT OF

THE FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ENTITLED

“HOMELAND THREATS AND AGENCY RESPONSES”

PRESENTED

NOVEMBER 14, 2013

Statement of
The Federal Bureau of Investigation
Before the
Committee on Homeland Security and Governmental Affairs
United States Senate
At a Hearing Entitled
"Homeland Threats and Agency Responses"
November 14, 2013

Introduction

Good morning, Chairman Carper, Ranking Member Coburn, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

Today's FBI is a threat-focused, intelligence-driven organization. Every FBI professional understands that preventing the key threats facing our nation means constantly striving to be more efficient and more effective.

Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and to our communities.

These diverse threats illustrate the complexity and breadth of the FBI's mission and make clear the importance of its partnerships. We cannot do it alone. To accomplish its mission, the FBI relies heavily upon its partners around the globe.

In fact, our national headquarters and local field offices have built partnerships with just about every federal, state, local, tribal, and territorial law enforcement agency in the nation. Our agents and professional staff also work closely with law enforcement, intelligence, and security services in foreign countries, as well as international organizations like Interpol.

By combining our resources and leveraging our collective expertise, we are able to investigate national security threats that cross both geographical and jurisdictional boundaries.

It is important to emphasize that the FBI carries out this broad mission with rigorous obedience to the rule of law and protecting the civil rights and civil liberties of the citizens we serve.

Counterterrorism

Counterterrorism remains our top priority. The FBI works with our law enforcement and Intelligence Community (IC) partners to integrate intelligence and operations, and to detect and disrupt terrorists and their organizations.

As the Boston bombings this past April illustrate, the terrorist threat against the United States remains very real. We face a continuing threat from homegrown extremists, especially those who act alone or in small cells. Homegrown Violent Extremists (HVEs) present unique challenges because they do not share a typical profile, and their experiences and motives are often distinct, which makes them difficult to identify and their plots difficult to disrupt. Al-Qa'ida and its affiliates continue to encourage extremists in the West to follow this model by engaging in individual violent attacks and have already incorporated the Boston bombings in their propaganda. The Boston Marathon bombing suspects are from the North Caucasus, but the links, if any, between the bombing and that region remain unclear. We currently assess the threat from North Caucasus-based militants to the Homeland to be minimal as they remain focused on fighting against Russian security forces in the North Caucasus.

The Boston bombing also demonstrated the devastating potential of an improvised explosive device (IED) crafted from simple components, which could inspire other extremists to use such tactics. The devices used in Boston were similar in design to instructions widely available online. In addition to the Boston attack, over the past two years we have also seen extremists attempt to detonate IEDs or bombs at such high profile targets as the Federal Reserve Bank in New York, the U.S. Capitol, and commercial establishments in downtown Chicago, Tampa, and Oakland. Fortunately, these attempts, as well as many other plots, were thwarted. Yet the threat remains.

Overseas, the terrorist threat is similarly complex and ever-changing. We are seeing more groups engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication. Al-Qa'ida and its affiliates, especially al-Qa'ida in the Arabian Peninsula (AQAP), continue to represent a top terrorist threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, the attempted bombing of U.S.-bound cargo planes in October of 2010, and a disrupted plot to conduct a suicide bomb attack on a U.S.-bound airliner in April 2012.

Beyond the Middle East, threats emanating from Africa remain a concern to the FBI. Al-Shabaab, based in Somalia, recently attacked the Westgate Mall in Nairobi, Kenya. The FBI continues to assess that al-Shabaab lacks the intent to conduct or directly support attacks in the United States, as doing so would not be consistent with the group's strategic aims of establishing an Islamic state in Somalia and defeating the Somali and foreign troops obstructing their efforts to do so. We expect Kenya to remain the primary focus of the group's external attacks, though other nearby countries participating in military offensives against the group, such as Ethiopia and Uganda, remain at risk as well. Nonetheless, the FBI remains concerned that externally focused elements affiliated with the group are likely to aspire to attack the West and the U.S. Additionally, domestic extremists could draw inspiration from the group's propaganda and the Westgate Mall attack to employ similar tactics in the Homeland.

In North Africa, al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) continues to grow its operational reach and safe haven into Libya, and Mali, threatening U.S. and Western interests in the region. The FBI assesses AQIM, its affiliates and allies, and aspirant groups in the region pose a low threat to the Homeland in the short- to mid-term, but pose a high threat to U.S. and Western interests in the region, especially at embassies, hotels, and diplomatic facilities in

Tunisia and Libya. Since 2009, AQIM has a demonstrated capability to target Western interests, most notably through kidnap for ransom techniques. Since 2011, AQIM splinter groups, along with Libya- and Tunisia-based Ansar al-Sharia extremists, have increasingly proven their anti-Western ideologies through high-profile attacks on the U.S. consulate in Benghazi, Libya, the U.S. Embassy in Tunis, Tunisia; British oil facilities in Algeria, and a French-owned mine in Arlit, Niger. Such attacks against U.S. interests will likely continue, especially as extremists continue to fight for autonomy and control against governments which they perceive are receiving assistance from the United States.

With respect to West Africa, the FBI assesses that Nigeria-based Boko Haram does not currently pose a threat to the Homeland. Boko Haram does, however, aspire to attack U.S. or Western interests in the region. Boko Haram demonstrated its capability for such attacks in its 2011 vehicle-borne IED attack on the United Nations headquarters in Abuja, Nigeria. Current counterterrorism pressure from Nigerian military and police forces has limited Boko Haram's ability to execute various operational plans against Western targets; however, communications, training, and weapons links between Boko Haram and AQIM, al-Shabaab, and AQAP, may strengthen Boko Haram's capacity to conduct terrorist attacks against U.S. or Western targets in the future.

To combat these threats, the FBI relies upon its 103 Joint Terrorism Task Forces (JTTFs) across the nation and 63 Legal Attache (LEGAT) Offices around the world. The FBI has added approximately 70 JTTFs since 9/11. Investigators, analysts, linguists, and SWAT experts from dozens of U.S. law enforcement and intelligence agencies comprise the JTTFs. The JTTFs serve as critical force multipliers that follow up on all terrorism leads, develop and investigate cases, and proactively identify threats and trends that may impact the region, the nation, and the world.

Since 9/11, JTTFs have been instrumental in breaking up cells like the "Portland Seven," the Northern Virginia jihad group, and the Daniel Patrick Boyd cell in North Carolina. They've foiled attacks against military institutions and personnel in New Jersey, New York, Maryland, Washington, Texas, and Virginia. They have disrupted plots against government and civilian targets across the country including the al-Qa'ida plot against the New York City Subway in 2009. They have traced sources of terrorist funding, responded to anthrax and other suspected weapons of mass destruction threats, halted the use of fake IDs, and arrested subjects who possessed deadly weapons and explosives.

To better address the evolving threat, the FBI has also established the Countering Violent Extremism (CVE) Office. This office leverages FBI resources and works with federal counterparts to empower our local partners to prevent violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the United States to commit acts of violence. The FBI is leading efforts to conduct outreach, and raise community awareness, while upholding civil rights and liberties.

Cyber Threats

The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas through cyber intrusions. This

threatens innovation and, as citizens, we are also increasingly vulnerable to losing our personal information. That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.

The FBI has built up substantial expertise to address cyber threats, both in the homeland and overseas.

Here at home, the FBI serves as the executive agent for the National Cyber Investigative Joint Task Force (NCIJTF) which joins together 19 intelligence, law enforcement, and military agencies to coordinate cyber threat investigations. The FBI works closely with our all our partners in the NCIJTF, including the National Security Agency (NSA) and the Department of Homeland Security (DHS). We have different responsibilities, but we must work together on cyber threat investigations to the extent of our authorities and share information among the three of us following the principle that notification of an intrusion to one agency will be notification to all.

While national-level coordination is important to securing the nation, teamwork at the local level is also essential. After more than a decade of combating cyber crime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners with many of the federal agencies that participate in the NCIJTF at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level.

Through the FBI's Legal Attache offices around the globe and partnerships with our international counterparts, we are sharing information and coordinating cyber investigations more than ever. We have Special Agents working alongside our foreign police department partners, they work to identify emerging trends and key players in the cyber crime arena.

It is important to note that we are also coordinating closely with our federal partners on the policy that drives our investigative efforts. Although our agencies have different roles, we also understand that we must work together on every significant intrusion and to share information among the three of us following the principle that notification of an intrusion to one agency will be notification to all.

In addition to cooperation within the government, there must be cooperation with the private sector. The private sector is the key player in cyber security. Private sector companies are the primary victims of cyber intrusions. And they also possess the information, the expertise, and the knowledge to address cyber intrusions and cyber crime in general. In February 2013, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing.

One example of an effective public-private partnership is the National Cyber Forensics and Training Alliance, a proven model for sharing private sector information in collaboration with law enforcement. Located in Pittsburgh, the Alliance includes more than 80 industry partners from a range of sectors, including financial services, telecommunications, retail and

manufacturing. The members of the Alliance work together with federal and international partners to provide real-time threat intelligence, every day.

Another initiative the FBI participates in, the Enduring Security Framework, includes top leaders from the private sector and the federal government. This partnership illustrates that the way forward on cyber security is not just about sharing information, but also about solving problems together.

We intend to build more bridges to the private sector in the cyber security realm. We must fuse private-sector information with information from the Intelligence Community and develop channels for sharing information and intelligence quickly and effectively.

In the last several years, the distribution of malicious software through networks of infected computers, or "botnets," by online criminals has emerged as a global cybersecurity threat. As a response, the FBI developed Operation Clean Slate, a broad team effort to address this significant threat. Operation Clean Slate is the FBI's comprehensive public/private approach to eliminate the most significant botnet activity and increase the practical consequences for those who use botnets for intellectual property theft, or other criminal activities.

In April 2013, the FBI implemented this plan and identified the Citadel Botnet as the highest priority botnet threat. Citadel is a type of malware known as a "Banking Trojan." This type of malicious software is designed to facilitate unauthorized access to computers to steal online banking credentials, credit card information, and other personally identifiable information (PII).

Focusing on the Citadel malware, Operation Clean Slate identified the specific actors: the coders who create the botnet, the herders who aggregate victim computers and the users who utilize the botnet. We also identified intended or actual victims of the botnet.

The FBI and its global partners then took action against Citadel. Through court ordered authorizations and leveraging industry partnerships, more than 1,400 controlling components of the botnet were disrupted, essentially ceasing its operations. Once these controlling components were rendered inoperable, it is estimated Operation Clean Slate freed more than 2.1 million robot computers from this malicious network.

The FBI must continue to develop and deploy creative solutions in order to defeat today's complex cyber threat actors. Instead of just building better defenses, we must also build better relationships, overcoming the obstacles that prevent us from sharing information and, most importantly, collaborating.

Active Shooter Threats

The recent shootings at the Navy Yard in Washington, D.C., the Los Angeles Airport, and the Westfield Garden State Plaza Mall, demonstrate that communities across America continue to face active shooter and mass casualty incidents. Since the Sandy Hook tragedy last December, the FBI has been working with the Department of Justice's Bureau of Justice Assistance to

provide tactical "active shooter" training to law enforcement agencies across the country. In conjunction with this training, the FBI and DOJ, working with our HHS, Education, and DHS partners, have developed an Active Shooter brochure and planning guides to complment this effort.

Over the past year, one hundred FBI agents have attended the Advanced Law Enforcement Rapid Response Training (ALERRT) school and trained other officers in life-saving tactics. The 16-hour Basic Active-Shooter course prepares first responders to isolate a threat, distract the threat actors, and end the threat. In addition, during the month of April, the FBI conducted two-day conferences and table top exercises with state, local, tribal, and campus law enforcement executives. The purpose of these conferences was to ensure that the ALERRT brought FBI field offices and law enforcement command staff together to discuss best practices and lessons learned from mass shooting incidents. We have hosted two-day conferences on active shooter situations at most of our 56 field offices nationwide followed by tabletop exercises based on real-life incidents.

These incidents have also given rise to collaboration among behavioral experts, victim assistance specialists, and other personnel to work through best practices, including how to best react to active shooter and mass casualty incidents. We are continuing our efforts with a new table top exercise specifically designed for campus law enforcement. This is an issue that impacts all of us, and the FBI is committed to working with our partners to protect our communities.

Conclusion

Chairman Carper, Ranking Member Coburn, I thank you for this opportunity to testify concerning the diverse threats facing the nation and the FBI's ongoing efforts to combat them. The FBI's efforts and successes would not have been possible without your support and the support of the American people. I would be happy to answer any questions you might have.