Department of Justice

STATEMENT OF

JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ENTITLED

"WORLDWIDE THREATS TO THE HOMELAND"

PRESENTED

SEPTEMBER 17, 2014

Statement of
James B. Comey
Director
Federal Bureau of Investigation
Department of Justice

Before the
Committee on Homeland Security
United States House of Representatives

Entitled
"Worldwide Threats to the Homeland"

Presented
September 17, 2014

Good morning, Chairman McCaul, Ranking Member Thompson, and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the FBI's efforts to combat threats against the Homeland.

Today's FBI is a threat-based, intelligence-driven organization. We live in a time of persistent terrorist and criminal threats to our national security, our economy, and to our communities. Just as our adversaries and threats continue to evolve, so, too, must the FBI. The key to this evolution lies with our greatest assets: our people and our partnerships. Every FBI professional understands that thwarting the threats facing our nation means constantly striving to be more effective and more efficient. The people of the FBI sacrifice much for their country, and I am proud to lead this organization of dedicated agents, analysts and professional staff.

To accomplish its mission, the FBI relies heavily upon its law enforcement and intelligence partners around the nation and around the globe.

By combining our resources and 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 resolute respect for privacy, confidentiality, civil rights and civil liberties of the citizens we serve.

Counterterrorism

Combating terrorism continues to be one of the top priorities for the FBI. As geopolitical conflict zones continue to emerge throughout many parts of the world, terrorist groups may use this instability to recruit and incite acts of violence.

While core al Qaeda isn't the dominant force it once was, we have seen the growth of the progeny of al Qaeda: Al Qaeda in the Islamic Maghreb, al Qaeda in the Arabian Peninsula, al-Nusra Front in Syria, and now ISIL in Iraq and Syria.

Syria remains at the forefront of our minds as the ongoing conflict shows no signs of subsiding. The continuing violence in both Syria and Iraq and the influx of foreign fighters threatens to further destabilize an already volatile region while also heightening the threat to the West. Due to the prolonged nature and the high visibility of the Syrian conflict, we are concerned that U.S. persons with an interest in committing violent extremist acts will continue to be drawn to the region. Foreign fighters traveling to Syria or Iraq could, for example, gain battlefield experience and increased exposure to violent extremist elements that may lead to further radicalization to violence; they may use these skills and exposure to radical ideology to return to their countries of origin, including the United States, to conduct attacks on the Homeland. The FBI is working closely with our domestic and international partners to track foreign fighters traveling to the Middle East and to disrupt them before they act.

The Islamic State of Iraq and the Levant (ISIL) remains committed to instilling fear and attracting recruits. ISIL has issued public statements confirming the terrorist organization's determination and dedication to globalterrorism. ISIL's widespread use of social media and growing online support intensified following the commencement of U.S. airstrikes in Iraq. ISIL has also shown the lengths to which it is willing to go to attract public attention. This was evident in the videos ISIL released depicting the beheadings of ISIL-held American hostages James Foley and Steven Sotloff. We are deeply concerned about the safety and security of American citizens worldwide, and ISIL and other foreign terrorist organizations may continue to try to capture American hostages in an attempt to force the U.S. government and people into making concessions that would only strengthen ISIL and further its terrorist operations

Al-Qa'ida in the Arabian Peninsula (AQAP) remains one of the greatest threats to the United States. AQAP's intent on carrying out violent acts against the West is still strong. Through AQAP's online English magazine *Inspire*, the group advocates simple and inexpensive lone wolf attacks against the Homeland and other Western targets. The first edition of *Inspire*, released in the summer of 2010, provided specific instructions on how to build a pipe bomb. Last month, AQAP released a new publication that further expanded upon these instructions to include building a pressure cooker bomb similar to the one used in the Boston Marathon bombing.

Here at home, we face a continued threat from homegrown violent extremists (HVEs). HVEs are individuals located in the United States who are inspired by terrorist ideology. These individuals present unique challenges because they do not share the profile of an identifiable group. Their experience and motives are often distinct, but they are increasingly savvy and willing to act

alone. They may gain inspiration from terrorist narratives, including material in English; events in the United States or abroad perceived as threatening to Muslims; the perceived success of other HVE plots, such as the November 2009 attack at Fort Hood; or their own grievances.

As you know, the FBI also relies heavily upon its 103 Joint Terrorism Task Forces (JTTFs) across the nation. The FBI has added approximately 70 JTTFs since 9/11. Investigators, analysts, linguists, and 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.

Finally, in an effort to better address the evolving threat, the Countering Violent Extremism (CVE) Office uses 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.

Today's FBI remains agile in its efforts to combat national security threats both here and abroad. We are committed to utilizing all of our resources to protect the citizens of this country, and we will continue to further our integration of operations and intelligence to prevent acts of terrorism.

Intelligence

The FBI is a national security and law enforcement organization that uses, collects, and shares intelligence in everything we do.

There was a time when the FBI was criticized for "working the inbox." Our work was driven by sources and the complaints that came to our door. We too often worked what was directly in front of us, which didn't always align with our biggest threats or allow us to look beyond the horizon.

Today we are constantly involved in a process of trying to understand the threats we face in each of our offices here and abroad – what's out there, what we see, what we might be missing. We gather intelligence, consistent with our authorities, to help us understand and rank those threats and to identify the intelligence gaps we face. We then try to fill those gaps and continue to learn as much as we can about the threats we are addressing and those we may need to address. We do this for national security and criminal threats, nationally and within each field office. We then compare the national and local perspectives to develop a threat prioritization ranking for each of the FBI's 56 Field Offices. By creating this ranking, we strive to actively pursue our highest threats. This gives us a better assessment of what the dangers are, what's being done about them, and what we should spend time on.

The FBI has come a long way in its intelligence transformation over the years, but there is always room to improve and grow. We have reinstituted the FBI's Intelligence Branch to elevate and expand the intelligence program. I am confident that this will result in a more robust FBI with continued integration of intelligence and operations. I also anticipate the expansion will

facilitate a smoother, more efficient exchange of intelligence with the Intelligence Community and international partners.

Cyber

We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our economy.

Given the scope of the cyber threat, agencies across the Federal government are making cyber security a top priority. The Department of Justice, including the FBI; the Department of Homeland Security; the National Security Agency and other U.S. Intelligence Community and law enforcement agencies have truly undertaken a whole-of-government effort to combat the cyber threat. Within the FBI, we are prioritizing the investigation and prevention of high-level intrusions against the United States, including the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We are working with our counterparts to predict and prevent attacks, rather than simply react after the fact.

FBI agents, analysts, and computer scientists use technical capabilities and traditional investigative techniques—such as sources and wiretaps, surveillance, and forensics—to fight cyber crime. We work side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and at the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24-hour cyber command center, CyWatch, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to Federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We also exchange information about cyber threats with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance (NCFTA).

We developed and recently deployed a malware repository and analysis system called Malware Investigator (MI) for intelligence and law enforcement partners. MI provides the FBI's domestic and foreign law enforcement partners as well as members of the Intelligence Community a way to submit malware directly to the FBI. This approach will enable the FBI to obtain a global view of the malware threat, while also providing the submitter technical information about the malware's functionality. Beyond technical reporting, MI identifies correlations that will allow users to "connect the dots" by highlighting instances in which malware was deployed in seemingly unrelated incidents. MI will be provided to FBI corporate and academic partners later this year, providing them a trusted venue in which to investigate, analyze, study and collaborate about malware threats.

In addition, our legal attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting and collaborating with newly established cyber crime centers at Interpol and Europol. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe

Over the past several months, the Justice Department has announced a series of separate indictments of overseas cyber criminals. In an unprecedented indictment in May, we charged five Chinese hackers with illegally penetrating the networks of six U.S. companies. The five members of China's People's Liberation Army allegedly used their illegal access to exfiltrate proprietary information, including trade secrets. Moreover, in June, charges were filed against Su Bin, a Chinese national, stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft.

Through the NCIJTF and in alliance with its U.S. government partners, international partners, and private sector stakeholders, the FBI has worked collaboratively in developing a multi-pronged effort aimed at defeating the world's most dangerous botnets. Over the past several years, the FBI's efforts to combat these significant cyber threats have caused the disruption and dismantlement of numerous botnets, including Butterfly Bot, Rove Digital, Coreflood, ZeroAccess, and GameOver Zeus, resulting in numerous arrests, extraditions, and convictions.

In addition to these recent investigative successes against the threat, we are continuing to work with our partners to prevent attacks before they occur. One area in which we have had great success with our overseas partners is in targeting infrastructure we believe has been used in distributed denial of service (DDoS) attacks, and preventing that infrastructure from being used for future attacks.

Since October 2012, the FBI and the Department of Homeland Security (DHS) have released more than 170,000 Internet Protocol addresses of computers that were believed to be infected with DDoS malware. We have released this information through Joint Indicator Bulletins (JIBs) to more than 130 countries via DHS's National Cybersecurity and Communications Integration Center (NCCIC), where our liaisons provide expert and technical advice for increased coordination and collaboration, as well as to our legal attachés overseas.

* * *

Chairman McCaul, Ranking Member Thompson, and the Committee, I thank you for this opportunity to testify concerning the diverse threats facing the nation and the FBI's ongoing efforts to combat them. I am now happy to answer any questions you might have.