Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"15 YEARS AFTER 9/11: THREATS TO THE HOMELAND"

PRESENTED
SEPTEMBER 27, 2016

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"15 YEARS AFTER 9/11: THREATS TO THE HOMELAND"

PRESENTED
SEPTEMBER 27, 2016

Good afternoon Chairman Johnson, Ranking Member Carper, and members of the Committee. Thank you for the opportunity to appear before you today to discuss the current threats to the homeland and our efforts to address new challenges. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. Our successes depend on interagency cooperation; among those partners are with me today; the Department of Homeland Security and the National Counterterrorism Center to address current and emerging threats.

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists are extremely dynamic. The tragic event in Orlando last June is a somber reminder of this threat. The FBI is leading a Federal terrorism investigation with the assistance of our State, local, and Federal partners. The ongoing investigation has developed strong indications of radicalization by this killer, but further investigation is needed to determine if this attack was inspired by a foreign terrorist organization. We are spending a tremendous amount of time trying to understand every moment of the killer's path, to understand his motives, and to understand the details of his life. We will continue to look forward in this investigation, and backward. Our work is very challenging. We are looking for needles in a nationwide haystack, but we are also called upon to figure out which pieces of hay might someday become needles. That is hard work and the particular challenge of identifying homegrown violent extremists.

These threats remain the highest priority and create the most serious challenges for the FBI, the U.S. Intelligence Community, and our foreign, State, and local partners. ISIL is relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. We continue to identify individuals who seek to join the ranks of foreign fighters

traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. In addition, we are confronting an explosion of terrorist propaganda and training available via the Internet and social networking media. Due to online recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the U.S. to recruit and carry out acts. Terrorists in ungoverned spaces—both physical and cyber—readily disseminate poisoned propaganda and training materials to attract easily influenced individuals around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change and transformation from the terrorist threat our nation faced a decade ago. ISIL's widespread reach through the Internet and social media is most concerning as the group has proven dangerously competent at employing such tools for its nefarious strategy. ISIL uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Recently released propaganda has included various English language publications circulated via social media.

Social media also helps groups such as ISIL to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable persons of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging. Echoing other terrorist groups, ISIL has advocated for lone offender attacks in Western countries. Recent ISIL videos and propaganda specifically advocate for attacks against soldiers, law enforcement, and intelligence community personnel. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters. We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old- fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in

technology to their advantage. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. When changes in technology hinder law enforcement`s ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States, including both physical and electronic surveillance. Physical surveillance is a critical and essential tool in detecting, disrupting, and preventing acts of terrorism, as well as gathering intelligence on those who are capable of doing harm to the nation. Along with our domestic and foreign partners, we are collecting and analyzing intelligence about the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing; in partnership with our many Federal, State, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the homeland.

Intelligence

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken two steps to improve this integration. First, we have established an Intelligence Branch within the FBI headed by an Executive Assistant Director ("EAD"). The EAD looks across the entire enterprise and drives integration. Second, we now have Special Agents and new Intelligence Analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better prepared to work well together in the field. Our goal every day is to get better at using, collecting and sharing intelligence to better understand and defeat our adversaries.

The FBI cannot be content to just work what is directly in front of us. We must also be able to understand the threats we face at home and abroad and how those threats may be connected. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps in what we know about these threats. We then seek to fill those gaps and learn as much as we can about the threats we are addressing and others on the threat landscape. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to organize threats into priority for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

Cyber

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to strike our critical infrastructure and to harm our economy.

The pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber-attacks as a top priority. Within the FBI, we are targeting the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets. We need to be able to move from reacting to such attacks after the fact to operationally preventing such attacks. That is a significant challenge, but one we embrace. As the committee is well aware, the frequency and impact of cyber-attacks on our nation’s private sector and government networks have increased dramatically in the past decade and are expected to continue to grow.

We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. For example, as the committee is aware, the Office of Personnel Management (OPM) discovered last year that a number of its systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective Federal government employees, as well as other individuals for whom a Federal background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

Another growing threat to businesses and individuals alike is Ransomware. Last year alone there was a reported loss of more than $24 million. The FBI works closely with the private

sector so that companies may make informed decisions in response to malware attacks. Companies can prevent and mitigate malware infection by utilizing appropriate back-up and malware detection and prevention systems, and training employees to be skeptical of emails, attachments, and websites they don't recognize. The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity, lead to other victimizations, or be used to facilitate serious crimes.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and sharing inside and outside of government, to our internal emphasis on developing and retaining new talent and changing the way we operate to evolve with the cyber threat. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States from all of those threats and the men and women of the Bureau continue to meet and exceed those expectations, every day. I want to thank them for their dedication and their service.

Chairman Johnson, Ranking Member Carper, and Committee members, I thank you for the opportunity to testify concerning the threats to the Homeland. I am happy to answer any questions you might have.