Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"WORLDWIDE THREATS TO THE HOMELAND: ISIS AND THE NEW WAVE OF TERROR"

PRESENTED
JULY 14, 2016

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"WORLDWIDE THREATS TO THE HOMELAND: ISIS AND THE NEW WAVE OF TERROR"

PRESENTED
JULY 14, 2016

Good afternoon Chairman McCaul, Ranking Member Thompson, 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 including terrorists' use of technology to both inspire and recruit. The widespread use of technology permits terrorists to propagate the persistent terrorist message to attack U.S. interests whether in the homeland or abroad. As the threat to harm our 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 with me today are the Department of Homeland Security and the National Counterterrorism Center with whom we work 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 threat 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 month 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 foreign terrorist organizations. 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. Our work is very challenging: We are looking for needles in a nationwide haystack, but even more challenging, we are also called upon to figure out which pieces of hay might someday become needles. That is hard work and it is 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. Terrorists 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 the individuals cannot travel, the terrorists 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 in furtherance of 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 is used as a tool for groups such as ISIL to spot and assess potential recruits. With greater access to social media platforms, terrorists can spot, assess, recruit and radicalize vulnerable persons of all ages in the United States either to travel to engage in terrorist organization activities or to conduct a homeland attack. Such use of the Internet, including social media, in furtherance of terrorism and other crimes must continue to be addressed by all lawful means, while respecting international obligations and commitments regarding human rights (including freedom of expression), the free flow of information, and a free and open Internet.

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, not necessarily with the initial intention to participate in terrorist activities. 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 in Western countries. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers. The challenge here is how to defeat ISIS and thwart its use of the Internet for terrorist and other criminal activity while continuing to help the Internet be a force for good that promotes the enjoyment of freedom of expression, association, and peaceful assembly – especially for individuals who are acutely at risk.

Some of these conversations occur openly on social networking sites, but others take place via private messaging platforms that use encryption. Terrorists' exploitation of encrypted platforms presents serious challenges to law enforcement's ability to identify, investigate, and

disrupt terrorist threats. We respect the 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, because the free flow of information is vital to a thriving democracy.

The United States believes that the Internet has been, and will be, a tremendous force for good – it has enabled the promotion and protection of fundamental freedoms. But the Internet's potential is dependent on people's ability and willingness to use it without undue restrictions and fear. Individuals must be able to trust that there will be respect for privacy, access to information, and freedom of expression, and there will be appropriate legal restraints on government action. Without these protections, the Internet risks becoming a mechanism for social control, rather than a place for all to express and exchange ideas, views, and information. The risks posed by terrorism are great, and the need for law enforcement is strong, but we must balance those requirements against the important role played by free expression in helping to address those same challenges.

The benefits of our increasingly digital lives, however, have been accompanied by new obstacles and, accordingly, we are considering 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. The decisions we make over the next several years about the future of the Internet --- including the laws and policies that are put in place to protect freedom of expression while thwarting terrorist and other criminal activities -- will determine whether our children will continue to enjoy an open, interoperable, secure and reliable Internet. And this in turn will greatly affect whether the Internet will continue to yield the remarkable social, economic and political progress that it has to date.

We must ensure both the 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, those changes also hinder efforts 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. 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. 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, and while we are making progress, we still have more work to do. Our goal every day is to get better at using, collecting, and sharing intelligence to better understand and defeat our adversaries.

We have established an Intelligence Branch within the FBI to lead integration across the organization, with responsibility for all intelligence strategy, resources, policies, and functions. The branch is headed by an Executive Assistant Director who looks across the entire enterprise and drives integration. We have also established a Bureau Intelligence Council within the Intelligence Branch to ensure we take a consolidated and integrated approach to threats. As part of this council, senior-level intelligence professionals will lead enterprise-wide strategic assessments, facilitate a broader understanding of how threats mitigated across operational programs are related, and help balance our priorities with those of the broader intelligence community and U.S. government.

We have also put in place training for all levels of the workforce, from entry-level employees to senior leaders, to ensure we achieve that integration throughout the enterprise. New agents and analysts now engage in practical training exercises and take core courses together at the FBI Academy — and, as a result, are better prepared to collaborate effectively throughout their careers. In addition, all field supervisory agents, supervisory analysts, and foreign language program managers, as well as headquarters unit chiefs, now attend a two-day forum focused on sharing best practices to advance integration. All section chiefs and GS-15 field agents and analysts also attend a two-and-a-half-day course on effectively integrating intelligence processes to maximize resources against prioritized threats. Finally, our entire executive management team at headquarters has participated in two integration sessions to ensure the integration of intelligence into every aspect of the FBI's work.

In addition, we are dedicated to expanding the developmental and leadership opportunities for all members of the intelligence program workforce. We recently put in place seven additional Senior Supervisory Intelligence Analyst positions in various offices around the country to increase leadership opportunities for our analyst cadre and enhance our management of field intelligence work. These GS-15 analysts manage intelligence in the field, fulfilling a

role that has traditionally been performed by agents and demonstrating we are promoting effective integration throughout the organization.

We have also redesigned the training curriculum for another part of the Intelligence Program workforce — Staff Operations Specialists ("SOSs") — to aid in their performance of tactical functions in the field. In addition, a new development model clearly identifies SOS work responsibilities, tasks, training, and opportunities at the basic, intermediate, and advanced levels to guide the professional growth of SOSs across the organization at all points throughout their FBI careers.

Similarly, our language workforce continues to make important contributions to the mission. Our language professionals have recently supported numerous important investigations and operations, including Malaysia Airlines Flight 17 last summer, numerous ISIL-related investigations, the disruption of a nuclear threat in Moldova, and so many others. The National Virtual Translation Center ("NVTC") also continues to provide excellent service, supporting hundreds of government offices each year.

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. Toward 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 priorities 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 and criminal threat the FBI faces is cyber-enabled in some way. We face sophisticated cyber threats from foreign intelligence agencies, hackers for hire, organized crime syndicates, and terrorists. These threat actors constantly seek to access and steal classified information, our trade secrets, our technology, and our ideas — things of incredible value to all of us and of great importance to our national and economic 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 Federal government view improving cyber security and preventing 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 organized crime syndicates, as well as the most prolific botnets. We need to

be able to move from reacting to such malicious activity after the fact to preventing such attacks. That is a significant challenge, but one we embrace.

As the committee is well aware, the frequency and impact of malicious cyber activity 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, which is malicious software that takes control of victims' computers and systems and encrypts the data until the victims pay a ransom. Last year alone reported losses from ransomware totaled more than $24 million. The FBI works closely with the private sector so that companies may make informed decisions in response to ransomware and other 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 encourage payment of ransom, as payment of extortion monies may encourage continued criminal activity and paying a ransom does not guarantee that an organization will regain access to its data.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and information sharing inside and outside of government, to our emphasis on developing and retaining new talent and changing the way we operate to defeat these threats. 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 McCaul, Ranking Member Thompson, 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.