Department of Justice

STATEMENT OF
NIKKI FLORIS
DEPUTY ASSISTANT DIRECTOR OF COUNTERTERRORISM
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"ADAPTING TO DEFEND THE HOMELAND AGAINST THE EVOLVING INTERNATIONAL TERRORIST THREAT"

PRESENTED
DECEMBER 6, 2017

STATEMENT OF
NIKKI FLORIS
DEPUTY ASSISTANT DIRECTOR OF COUNTERTERRORISM
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"ADAPTING TO DEFEND THE HOMELAND AGAINST THE EVOLVING INTERNATIONAL THREAT"

PRESENTED
DECEMBER 6, 2017

Good morning Chairman Johnson, Ranking Member McCaskill, and members of the committee. Thank you for the opportunity to appear before you today to discuss the evolving terrorist threat to the homeland. As technology advances so, too, does terrorists' use of technology to communicate — both to inspire and recruit. Their widespread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the Homeland or abroad. As these threats to Western interests evolve, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships.

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. From a threat perspective, we are concerned with three areas in particular: (1) those who are inspired by terrorist propaganda and act out in support; (2) those who are enabled to act after gaining inspiration from violent extremist propaganda and communicating with members of foreign terrorist organizations who provide guidance on operational planning or targets; and (3) those who are directed by members of foreign terrorist organizations to commit specific, directed acts in support of the group's ideology or cause. Prospective terrorists can fall into any one of these three categories or span across them, but in the end the result is the same — innocent men, women, and children killed and families, friends, and whole communities left to struggle in the aftermath.

Currently, the FBI views the Islamic State of Iraq and Syria ("ISIS") and homegrown violent extremists as the main terrorism threats to the United States. ISIS is relentless and ruthless in its campaign of violence and has aggressively promoted its hateful message, attracting like-minded extremists. The threats posed by foreign terrorist fighters, including those recruited from the United States, are extremely dynamic. 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. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, as well as homegrown violent extremists who may

aspire to attack the United States from within. In addition, we are working to expose, refute and combat terrorist propaganda and training available via the Internet and social media networks. Due to online recruitment and indoctrination, foreign terrorist organizations are no longer solely dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts. Terrorists in ungoverned spaces—both physical and cyber—readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. They encourage these individuals to travel, or they motivate them to act at home. This is a significant transformation from the terrorist threat our nation faced a decade ago.

ISIS was able to construct a narrative that touched on many facets of life, from career opportunities to family life to a sense of community. Those messages were not tailored solely for those who are expressing signs of radicalization to violence —many who click through the Internet every day, receive social media push notifications, and participate in social networks have viewed ISIS propaganda. Ultimately, a lot of the individuals drawn to ISIS seek a sense of belonging. Echoing other terrorist groups, ISIS has advocated for lone offender attacks in Western countries. ISIS videos and propaganda have specifically advocated for attacks against soldiers, law enforcement, and intelligence community personnel, but have branched out to include any civilian as a worthy target.

Many foreign terrorist organizations use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to violent extremist messages, however, no group has been as successful at drawing people into its perverse ideology as ISIS. ISIS has proven dangerously competent at employing such tools for its nefarious strategy. ISIS uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Social media hijacked by groups such as ISIS to spot and assess potential recruits. With the widespread use of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the United States either to travel or to conduct a homeland attack. Through the Internet, terrorists overseas now have access into our local communities to target and recruit our citizens and spread the message of radicalization to violence faster than we imagined just a few years ago.

ISIS is not the only terrorist group of concern. Al Qaeda maintains its desire for large-scale spectacular attacks; however, continued CT pressure has degraded the group, and in the near term, al Qaeda is more likely to focus on supporting small-scale, readily achievable attacks against U.S. and allied interests in the Afghanistan/Pakistan region. Simultaneously, over the last year, propaganda from al Qaeda leaders seeks to inspire individuals to conduct their own attacks in the United States and the West.

As the threat to harm the United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence concerning the ongoing threat posed by foreign

terrorist organizations and homegrown violent extremists. We continue to encourage information sharing, which is evidenced through our partnerships with many Federal, State, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to help stay ahead of these threats.

Unfortunately, the rapid pace of advances in mobile and other communication technologies continues to present a significant challenge to conducting lawful court-ordered access to digital information or evidence, whether that information is being electronically transmitted over networks or at rest on a device or other form of electronic storage. There is a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so. The FBI refers to this growing challenge as "Going Dark," and it affects the spectrum of our work. In the counterterrorism context, for instance, our agents and analysts are increasingly finding that communications and contacts between groups like ISIS and potential recruits occur in encrypted private messaging platforms.

The exploitation of encrypted platforms presents serious challenges to law enforcement's ability to identify, investigate, and disrupt threats that range from counterterrorism to child exploitation, gangs, drug traffickers and white-collar crimes. In addition, 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 effects on our ability to identify, stop, and prosecute these offenders. In fiscal year 2017, the FBI was unable to access the content of approximately 7800 mobile devices using appropriate and available technical tools, even though there was legal authority to do so. This figure represents slightly over half of all the mobile devices the FBI attempted to access in that timeframe.

When possible and legally permissible, our agents develop investigative workarounds on a case-by-case basis, including by using physical world techniques and examining non-content sources of digital information (such as metadata). As an organization, the FBI also invests in alternative methods of lawful engineered access. Ultimately, these efforts, while significant, have severe constraints. Non-content information, such as metadata, is often simply not sufficient to meet the rigorous constitutional burden to prove crimes beyond a reasonable doubt. Developing alternative technical methods is typically a time-consuming, expensive, and uncertain process. Even when possible, such methods are difficult to scale across investigations, and may be perishable due to a short technical lifecycle or as a consequence of disclosure through legal proceedings.

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. Our aim is not to expand the government's surveillance authority, but rather to ensure that we can obtain

electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe. The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have seen how criminals and terrorists use advances in technology to their advantage. 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 criminals or terrorists.

Some observers have conceived of this challenge as a trade-off between privacy and security. In our view, the demanding requirements to obtain legal authority to access data—such as by applying to a court for a warrant or a wiretap—necessarily already account for both privacy and security. The FBI is actively engaged with relevant stakeholders, including companies providing technological services, to educate them on the corrosive effects of the Going Dark challenge on both public safety and the rule of law, and with the academic community and technologists to work on technical solutions to this problem.

Also, as this Committee is aware, section 702 of the Foreign Intelligence Surveillance Act ("FISA"), is due to sunset at the end of this year. Section 702 is a critical tool that the intelligence community uses properly to target non-U.S. persons located outside the United States to acquire information vital to our national security. To protect privacy and civil liberties, this program has operated under strict rules and has been carefully overseen by all three branches of the government. Given the importance of section 702 to the safety and security of the American people, the Administration urges Congress to permanently reauthorize title VII of FISA.

Conclusion

Chairman Johnson, Ranking Member McCaskill, and committee members, I thank you for the opportunity to testify concerning the evolving threats to the Homeland and the challenges we face in confronting the threat. We are grateful for the support that you and this Committee have provided to the FBI. I am happy to answer any questions you might have.