Department of Justice

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
SEPTEMBER 27, 2017

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
SEPTEMBER 27, 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 current threats to the homeland. Our Nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists to cyber criminals to hostile foreign intelligence services and operatives. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must also be able to stay current with constantly changing and new technologies that make our jobs both easier and harder. Our adversaries – terrorists, foreign intelligence services, and criminals – take advantage of such modern technology to hide their communications, recruit followers, plan and encourage espionage, cyber attacks or terrorism, to disperse information on different methods to attack the U.S. homeland, and to facilitate other illegal activities. As these threats evolve, we must adapt and confront these 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 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 has designated the Islamic State of Iraq and ash-Sham ("ISIS") and homegrown violent extremists as the main terrorism threats to the Homeland. 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 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 confronting a surge in 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 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.

Unlike other groups, ISIS 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 signs 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 the individuals drawn to ISIS seek a sense of belonging. Echoing other terrorist groups, ISIS has advocated for lone offender attacks in Western countries. Recent ISIS videos and propaganda specifically advocate for attacks against soldiers, law enforcement, and intelligence community personnel.

Many foreign terrorist organizations use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to 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 also helps groups such as ISIS to spot and assess potential recruits. With the widespread distribution 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 direct access into our local communities to target and recruit our citizens and spread the message of radicalization faster than we imagined just a few years ago.

ISIS is not the only terrorist group of concern. Al-Qa'ida maintains its desire for large-scale spectacular attacks, however continued CT pressure has degraded the group, and in the near term al-Qa'ida 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-Qa'ida leaders seeks to inspire individuals to conduct their own attacks in the United States and the West.

In addition to foreign terrorist organizations, domestic extremist movements collectively pose a steady threat of violence and economic harm to the United States. Some trends within individual movements will shift as most drivers for domestic extremism, such as perceptions of government or law enforcement overreach, socio-political conditions, and reactions to legislative actions, remain constant. We are most concerned about the lone offender attacks, primarily shootings, as they have served as the dominant mode for lethal domestic extremist violence. We anticipate law enforcement, racial minorities, and the U.S. Government will continue to be significant targets for many domestic extremist movements.

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 threats to the homeland.

Intelligence

Integrating intelligence in all we do remains a critical strategic pillar of the FBI strategy. The constant evolution of the FBI's intelligence program will help us address the ever-changing threat environment. We must constantly update our intelligence apparatus to improve the way we use, collect, and share intelligence to better understand and defeat our adversaries. We cannot be content to only work the matters directly in front of us. We must also look beyond the horizon to understand the threats we face at home and abroad and how those threats may be connected.

To that end, we gather intelligence, consistent with our authorities, to help us understand and prioritize identified threats, to reveal the gaps in what we know about these threats, and to fill those gaps. 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 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.

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade to improve our understanding and mitigation of threats. Over the past few years, we have taken several steps to improve this integration. First, we established an Intelligence Branch within the FBI, headed by an Executive Assistant Director who drives integration across the enterprise. We also developed and implemented a series of

integration-focused forums that ensure all members of our workforce understand and internalize the importance of intelligence integration. We now train our Special Agents and Intelligence Analysts together at the FBI Academy where they engage in joint training exercises and take core courses together prior to their field deployments. As a result, they are better prepared to integrate their skillsets in the field. Additionally, our training forums for executives and frontline supervisors continue to ensure our leaders are informed about our latest intelligence capabilities and allow them to share best practices for achieving intelligence integration.

I also urge the Congress to renew section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which 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 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 reauthorize title VII of FISA without a sunset provision._

Counterintelligence

The Nation faces a rising threat, both traditional and asymmetric, from hostile foreign intelligence services and their proxies. Traditional espionage, often characterized by career foreign intelligence officers acting as diplomats or ordinary citizens, and asymmetric espionage, often carried out by students, researchers, or businesspeople operating front companies, is prevalent. Foreign intelligence services not only seek our Nation's state and military secrets, but they also target commercial trade secrets, research and development, and intellectual property, as well as insider information from the Federal Government, U.S. corporations, and American universities. Foreign intelligence services and other state-directed actors continue to employ more creative and more sophisticated methods to steal innovative technology, critical research and development data, and intellectual property, in an effort to erode America's economic leading edge. These illicit activities pose a significant threat to national security and continue to be a priority and focus of the FBI.

Our counterintelligence efforts are also aimed at the growing scope of the insider threat — that is, when trusted employees and contractors use their legitimate access to steal secrets for personal benefit or to benefit a company or another country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations. We are also investigating media leaks, when insiders violate the law and betray the nation's trust by selectively leaking classified information, sometimes mixed with disinformation, to manipulate the public and advance their personal agendas.

In addition to the insider threat, the FBI has focused on a coordinated approach across divisions that leverages both our classic counterespionage tradecraft and our technical expertise

to more effectively identify, pursue, and defeat hostile state actors using cyber means to penetrate or disrupt U.S. Government entities or economic interests.

Finally, we have initiated a media campaign to increase awareness of the threat of economic espionage. As part of this initiative, we have made a threat awareness video, titled "The Company Man," available on our public website, which has been shown thousands of times to raise awareness and generate referrals from the private sector.

Cyber

Virtually every national security and criminal threat the FBI faces is cyber-based or technologically facilitated. 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 our nation's classified information, trade secrets, technology, and ideas — all of which are of great importance to our national and economic security. They seek to strike our critical infrastructure and to harm our economy.

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. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as other technically sophisticated attacks.

Botnets used by cyber criminals are one example of this trend and have been responsible for billions of dollars in damages over the past several years. The widespread availability of malicious software (malware) that can create botnets allows individuals to leverage the combined bandwidth of thousands, if not millions, of compromised computers, servers, or network-ready devices to conduct attacks. Cyber threat actors have also increasingly conducted ransomware attacks against U.S. systems, encrypting data and rendering systems unusable – victimizing individuals, businesses, and even public health providers.

Cyber threats are not only increasing in scope and scale, they are also becoming increasingly difficult to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that can be used to facilitate cyber attacks. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient. Additionally, many cyber actors are based abroad or obfuscate their identities by using foreign infrastructure, making coordination with international law enforcement partners essential.

The FBI is engaged in a myriad of efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of government, to developing and retaining new talent, to examining the way we operate to disrupt and 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.

Going Dark

The rapid pace of advances in mobile and other communication technologies continues to present a significant challenge to conducting court-ordered electronic surveillance of criminals and terrorists. Unfortunately, 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. 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 terrorists who are using social media to recruit, plan, and execute an attack in our country.

In the criminal context, 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. In the first 10 months of this fiscal year, the FBI was unable to access the content of more than 6,000 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.

Where at all possible, 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.

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.

Weapons of Mass Destruction

The FBI, along with its U.S. Government partners, is committed to countering the Weapons of Mass Destruction ("WMD") threat (*e.g.*, chemical, biological, radiological, nuclear) and preventing terrorist groups and lone offenders from acquiring these materials either domestically or internationally.

Domestically, the FBI's counter-WMD threat program, in collaboration with our U.S. Government partners, prepares for and responds to WMD threats (*e.g.*, investigate, detect, search, locate, diagnostics, stabilization, and render safe WMD threats). Internationally, the FBI, in cooperation with our U.S. partners, provides investigative and technical assistance as well as capacity-building programs to enhance our foreign partners' ability to detect, investigate, and prosecute WMD threats.

Conclusion

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 McCaskill, 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.