Department of Justice

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
OCTOBER 10, 2018

STATEMENTOF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

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

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
OCTOBER 10, 2018

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 United States Homeland. Our Nation continues to face a multitude of serious and evolving threats ranging from Homegrown Violent Extremists (HVEs) to cyber criminals to hostile foreign intelligence services and operatives. Keeping pace with these threats is a significant challenge for the FBI. Our adversaries – terrorists, foreign intelligence services, and criminals – take advantage of modern technology to: hide their communications; recruit followers; and 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

The threat posed by terrorism – both International Terrorism (IT) and Domestic Terrorism (DT) – has evolved significantly since 9/11. Preventing terrorist attacks remains the FBI's top priority. We face persistent threats to the Homeland and to U.S. interests abroad from HVEs, domestic terrorists, and Foreign Terrorist Organizations (FTOs). The IT threat to the U.S. has expanded from sophisticated, externally directed FTO plots to include individual attacks carried out by HVEs who are inspired by designated terrorist organizations. We remain concerned that groups such as the Islamic State of Iraq and ash-Sham (ISIS) and al-Qa'ida (AQ) have the intent to carry out large-scale attacks in the U.S.

The FBI assesses HVEs are the greatest terrorism threat to the Homeland. These individuals are global jihad-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized direction from FTOs. We, along with our law enforcement partners, face significant challenges in identifying and disrupting HVEs.

This is due, in part, to their lack of a direct connection with an FTO, an ability to rapidly mobilize, and the use of encrypted communications.

In recent years, prolific use of social media by FTOs has greatly increased their ability to disseminate their messages. We have also been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment and indoctrination, FTOs are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts of terrorism. 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 motivate these individuals to act at home or encourage them to travel. This is a significant transformation from the terrorist threat our Nation faced a decade ago.

Despite significant losses of territory, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded extremists. Unlike other groups, ISIS has constructed a narrative that touches on all facets of life, from family life to providing career opportunities to creating a sense of community. The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who click through the Internet every day, receive social media 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 have specifically advocated 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, who has proven dangerously competent at employing such tools. ISIS uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the U.S. either to travel or to conduct an attack on the Homeland. Through the Internet, terrorists overseas now have direct access to our local communities to target and recruit our citizens and spread the message of radicalization faster than was imagined just a few years ago.

The threats posed by foreign fighters, including those recruited from the U.S., are very dynamic. We will continue working to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, those foreign fighters who may attempt to return to the United States, and HVEs who may aspire to attack the United States from within.

ISIS is not the only terrorist group of concern. Al-Qa'ida maintains its desire for large-scale spectacular attacks. However, continued counterterrorism 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 U.S. and the West.

In addition to FTOs, domestic extremist movements collectively pose a steady threat of violence and economic harm to the United States. Trends within individual movements may shift, but the underlying drivers for domestic extremism – such as perceptions of government or law enforcement overreach, socio-political conditions, and reactions to legislative actions – remain constant. The FBI is most concerned about 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 U.S. and our interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. The FBI uses all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we collect and analyze 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. The FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to stay ahead of threats to the Homeland.

Intelligence

Incorporating 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 collect, use, and share intelligence to better understand and defeat our adversaries. We cannot be content only to 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. We must also ensure we are providing our partners, whether in the public or private sectors, with actionable, relevant intelligence to help them address their own unique threats.

To that end, The FBI gathers intelligence, pursuant to legal 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 national and local field office levels. 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 is being done about them, and where we should prioritize our resources.

Given the fast pace of technological evolution, we must also focus on ensuring our information technology capabilities allow us to collect and assess information as quickly and thoroughly as possible. We must continue to deploy superior technological capabilities and solutions for large data sets, such as those derived from digital media.

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. The FBI's Intelligence Branch, created in August 2014, provides strategic direction and oversight of the FBI's Intelligence Program and is responsible for intelligence strategy, resources, policies, and operations. Our Special Agents and Intelligence Analysts train 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. To build on the Quantico-based training, the FBI now offers significant follow-on training courses that integrate Special Agents, Intelligence Analysts, Staff Operations Specialists, and Language Analysts. Additionally, our training forums for executives and front line supervisors continue to ensure our leaders are informed about our latest intelligence capabilities and allow them to share best practices for achieving intelligence integration.

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, are 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 federal employees and contractors 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.

We have also continued our engagement with the private sector and academia on the threat of economic espionage and technology transfer. We have addressed national business and academic groups, met with individual companies and university leaders, worked with sector-specific groups, and encouraged all field offices to maintain close, ongoing liaison with entities across the country that have valuable technology, data, or other assets.

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 U.S. 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, which 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, and 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 by encrypting data and rendering systems unusable, thereby victimizing individuals, businesses, and even public health providers.

Cyber threats are not only increasing in scope and scale, but 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

"Going Dark" describes circumstances where law enforcement is unable to obtain critical information in an intelligible and usable form (or at all), despite having a court order authorizing the government's access to that information. As a technical matter, this challenge extends across several products and platforms, whether it involves "data at rest," such as on a physical device, or "data in motion," as with real-time electronic communications.

Going Dark remains a serious problem for the FBI across our investigative areas, from counterterrorism to child exploitation, gangs, drug traffickers, and white collar crimes. The inability to access evidence or intelligence despite the lawful authority to do so significantly impacts the FBI's ability to identify, investigate, prosecute, or otherwise deter criminals, terrorists, and other offenders.

Our Federal, State, local, and international law enforcement partners face similar challenges in maintaining access to electronic evidence despite having legal authorization to do so. Indeed, within the last few months, the Nation's sheriffs called for "the U.S. Congress to exercise leadership in the Nation's public safety interest" to address the Going Dark challenge. Several of our closest law enforcement and intelligence partners (the United Kingdom, Canada, Australia, and New Zealand) similarly described this as a "pressing international concern that requires urgent, sustained attention and informed discussion."

The FBI recognizes the complexity of the issue, but we believe there is a tremendous opportunity for responsible stakeholders to work together to find sustainable solutions that preserve cybersecurity and promote public safety.

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 explosives) by preventing terrorist groups and lone offenders from acquiring these materials either domestically or internationally through preventing nation state proliferation of WMD sensitive technologies and expertise.

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, diagnose, stabilize, 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.

Countering Unmanned Aircraft Systems (C-UAS)

The threat from Unmanned Aircraft Systems in the U.S. is steadily escalating. While we are working with FAA and other agencies to safely integrate UAS into the national airspace system, the FBI assesses with high confidence that terrorists overseas will continue to use small UAS to advance nefarious activities and exploit physical protective measures. While there has been no successful malicious use of UAS by terrorists in the United States to date, terrorist groups could easily export their battlefield experiences to use weaponized UAS outside the conflict zone. We have seen repeated and dedicated efforts to use UAS as weapons, not only by terrorist organizations, such as ISIS and Al Qa'ida, but also by transnational criminal organizations such as MS-13 and Mexican drug cartels, which may encourage use of this technique in the U.S. to conduct attacks. The FBI assesses that, given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering. This risk has only increased in light of the publicity associated with the apparent attempted assassination of Venezuelan President Maduro using explosives-laden UAS.

The FBI recently disrupted a plan in the United States to use drones to attack the Pentagon and the Capitol building. On November 1, 2012, Rezwan Ferdaus was sentenced to 17 years in federal prison for attempting to conduct a terrorist attack and providing support to al-Qa'ida. Ferdaus, who held a degree in physics, obtained multiple jet-powered, remote-controlled model aircraft capable of flying 100 miles per hour. He planned to fill the aircraft with explosives and crash them into the Pentagon and the Capitol using a GPS system in each aircraft. Fortunately, the FBI interrupted the plot after learning of it and deploying an undercover agent.

Last week, thanks in large part to the outstanding leadership of this Committee, the FBI and DOJ received new authorities to deal with the UAS threat in the *FAA Reauthorization Act of 2018*. That legislation enables the FBI to counter UAS threats while safeguarding privacy and promoting the safety and efficiency of the national airspace system. The FBI is grateful to the Chairman, the Ranking Member, and other members of this Committee for championing this critical authority.

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 the FBI to protect the United States from all of those threats, and the men and women of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

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