Department of Justice

STATEMENT OF

CHRISTOPHER 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
NOVEMBER 5, 2019

STATEMENT OF
CHRISTOPHER 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
NOVEMBER 5, 2019

Good afternoon Chairman Johnson, Ranking Member Peters, 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, conduct 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.

Just as our adversaries evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and indeed our communities. These diverse threats underscore the complexity and breadth of the FBI's mission: to protect the American people and uphold the Constitution of the United States.

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. However, the threat posed by terrorism — both international terrorism ("IT") and domestic violent extremism — has evolved significantly since 9/11.

The most persistent threats to the Nation and to U.S. interests abroad are homegrown violent extremists ("HVEs"), domestic violent extremists, 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 Qaeda have the intent to carry out large-scale attacks in the U.S.

The FBI assesses HVEs are the greatest, most immediate terrorism threat to the homeland. These individuals are FTO-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 enhanced their ability to disseminate messages. We have also been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment, indoctrination, and instruction, 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 virtual — 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 their territorial defeat in Iraq and Syria, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded violent extremists. The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who enter messaging apps 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 violent terrorist messages. However, no group has been as successful at drawing people into its perverse ideology as ISIS, which has proven dangerously competent at employing such tools. ISIS uses traditional media platforms as well as widespread social media campaigns to propagate its 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 to foreign lands or to conduct an attack on the homeland. Through the Internet, terrorists anywhere overseas now have direct access to our local communities to target and recruit our citizens and spread their message 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 Qaeda maintains its desire for large-scale, spectacular attacks. While, continued counterterrorism pressure has degraded the group's Afghanistan-Pakistan senior leadership, in the near term, al Qaeda is more likely to focus on building its international affiliates and supporting small-scale, readily achievable attacks in key regions such as east and west Africa. Simultaneously, over the last year, propaganda from al Qaeda leaders seeks to inspire individuals to conduct their own attacks in the U.S. and the West.

In addition to FTOs, domestic violent extremists collectively pose a steady threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism — such as perceptions of government or law enforcement overreach, socio-political conditions, racism, anti-Semitism, Islamophobia, 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 lethal mode for domestic violent extremist attacks. More deaths were caused by domestic violent extremists than international terrorists in recent years.

The recent attacks in Texas and California underscore the continued threat posed by domestic violent extremists and perpetrators of hate crimes. Such crimes are not limited to the United States and, with the aid of Internet like-minded hate groups, can reach across borders. To combat the threat at home, the FBI established the Domestic Terrorism-Hate Crimes Fusion Cell, in spring 2019. Composed of subject matter experts from both the Criminal Investigative and Counterterrorism Divisions, the fusion cell offers program coordination from FBI Headquarters, helps ensure seamless information sharing across divisions, and augments investigative resources.

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 uses 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.

Counterintelligence

The Nation faces a continuing threat, both traditional and asymmetric, from hostile foreign intelligence agencies. Traditional espionage, often characterized by career foreign intelligence officers acting as diplomats or ordinary citizens, and asymmetric espionage, typically 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 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.

Foreign influence operations — which may include covert actions by foreign governments to influence U.S. policy decisions, political sentiment or public discourse — are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. The goal of these foreign influence operations directed against the United States is to spread disinformation, sow discord, push foreign nations' policy agendas, and ultimately undermine confidence in our democratic institutions and values. Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States — to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions. However, other influence operations may include targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft; criminal efforts to suppress voting and provide illegal campaign financing; concealing efforts to influence U.S. government activities, cyber attacks against voting infrastructure, along with computer intrusions targeting elected officials and others; and a whole slew of other kinds of influence, like both overtly and covertly manipulating news stories, spreading disinformation, leveraging economic resources, and escalating divisive issues.

Almost two years ago, I established the Foreign Influence Task Force ("FITF") to identify and counteract malign foreign influence operations targeting the United States. The FITF is uniquely positioned to combat this threat. The task force now brings together the FBI's expertise across the waterfront — counterintelligence, cyber, criminal, and even counterterrorism — to root out and respond to foreign influence operations. Task force personnel work closely with other U.S. government agencies and international partners concerned about foreign influence efforts aimed at their countries, using three key pillars.

Currently there are open investigations with a foreign influence nexus spanning FBI field offices across the country. Second, we are focused on information and intelligence-sharing. The FBI is working closely with partners in the Intelligence Community and in the federal government, as well as with State and local partners, to establish a common operating picture. The FITF is also working with international partners to exchange intelligence and strategies for combating what is a shared threat. The third pillar of our approach is based on strong relationships with the private sector. Technology companies have a front-line responsibility to secure their own networks, products, and platforms. But the FBI is doing its part by providing actionable intelligence to better enable the private sector to address abuse of their platforms by foreign actors. Over the last year, the FBI has met with top social media and technology

companies several times, provided them with classified briefings, and shared specific threat indicators and account information, so they can better monitor their own platforms.

But this is not just an election-cycle threat. Our adversaries are continuously trying to undermine our country, whether it is election season or not. As a result, the FBI must remain vigilant.

In addition to the threat posed by foreign influence, the FBI is also concerned about foreign investment by hostile nation states. Over the course of the last seven years, foreign investment in the U.S. has more than doubled. Concurrent with this growth, foreign direct investment ("FDI") in the U.S. has increasingly become a national security concern, as hostile nations leverage FDI to buy U.S. assets that will advance their intelligence, military, technology, and economic goals at the expense of U.S. national security. The Committee on Foreign Investment in the U.S. ("CFIUS"), an Executive Branch committee chaired by the Department of Treasury, was statutorily created to address potential risks to U.S. national security resulting from foreign acquisitions or mergers with U.S. companies. As part of this process, the FBI provides input and analysis to the National Intelligence Council within eight days of a CFIUS filing and a risk assessment to the Department of Justice within 30 days of a CFIUS filing. As a result of the Foreign Investment Risk Review Modernization Act ("FIRRMA"), which was enacted last year, the FBI anticipates its workload to increase dramatically.

Cyber Threats

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, these actors seek to steal our state secrets, our trade secrets, our technology, and the most intimate data about our citizens — 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 hold our critical infrastructure at risk, to harm our economy and to constrain our free speech.

As the Committee is well aware, the frequency and severity of malicious cyber activity on our Nation's private sector and government networks have increased dramatically in the past decade when measured by the amount of corporate data stolen or deleted, the volume of personally identifiable information compromised, or the remediation costs incurred by U.S. victims. We expect this trend to continue. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers, global organized crime syndicates, and other technically sophisticated and dangerous actors. FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques — such as sources, court- authorized electronic surveillance, physical surveillance, and forensics — to counter these threats. We continue to actively coordinate with our private and public partners to pierce the veil of anonymity surrounding cyber based crimes.

Botnets used by cyber criminals 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 disrupt the day-to-day activities of governments, businesses, and individual Americans. Cyber threat actors have also increasingly conducted ransomware attacks against U.S. systems, encrypting data and rendering systems unusable — thereby victimizing individuals, businesses, and even emergency service and public health providers.

Cyber threats are not only increasing in size and scope, but are also becoming increasingly difficult and resource-intensive to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that lower the barrier to entry for aspiring criminals and that can be used to facilitate malicious cyber activity. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient to disruption than ever. In addition, whether located at home or abroad, many cyber actors are obfuscating their identities and obscuring their activity by using combinations of leased and compromised infrastructure in domestic and foreign jurisdictions. Such tactics make coordination with all of our partners, including 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 the 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.

Conclusion

In closing, the work being done by the FBI is immeasurable; however, we cannot afford to be complacent. We must seek out new technologies and solutions for the problems that exist today as well as those that are on the horizon. We must build toward the future so that we are prepared to deal with the threats we will face at home and abroad and understand how those threats may be connected.

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you again for this opportunity to discuss the FBI's efforts to combat the myriad of threats it faces. I appreciate your continued support and look forward to answering any questions you might have.