Department of Justice

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

DECEMBER 7, 2017

STATEMENT OF
CHRISTOPHER A. WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"OVERSIGHT OF THE FBI"

DECEMBER 7, 2017

Good morning Chairman Goodlatte, Ranking Member Nadler, and members of the Committee. Thank you for this opportunity to discuss the FBI's programs and priorities for the coming year. On behalf of the men and women of the FBI, let me begin by thanking you for your ongoing support of the Bureau. We pledge to be the best possible stewards of the authorities and the funding you have provided for us, and to use them to maximum effect to carry out our mission.

Today's FBI is a global, threat-focused, intelligence-driven organization. Each FBI employee understands that, to defeat the key threats facing our nation, we must constantly strive to be more efficient, effective, and prescient.. Just as our adversaries continue to evolve, so must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and our communities. These diverse threats underscore the complexity and breadth of the FBI's mission.

We remain focused on defending the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting privacy, civil rights and civil liberties; and providing leadership and criminal justice services to Federal, State, tribal, municipal, and international agencies and partners. Our continued ability to carry out this demanding mission reflects the support and oversight provided by this Committee.

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.

National Security

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 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 violent extremists. The threats posed by ISIS foreign terrorist fighters, including those recruited from the U.S., 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.

The Internet is only one tool of many that terrorists use to recruit. However, 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 violent extremist ideology. Social media is 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-Qa'ida maintains its desire for large-scale attacks, however continued counter-terrorist (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 however, and especially 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 violent 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 violent 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 one lone offender attacks, primarily shootings, as they have served as the dominant mode for lethal domestic extremist violence. We anticipate that law enforcement, racial minorities, and the U.S. government will continue to be significant targets for many domestic violent 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 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.

Going Dark

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 is at rest on a device or other form of electronic storage. 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.

The benefits of our increasingly digital lives have been accompanied by new dangers, and we have seen how criminals and terrorists use advances in technology to their advantage. 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 also 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.

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.

We respect the right of people to engage in private communications, regardless of the medium or technology. 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. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private, because the free flow of information is vital to a thriving democracy. Our aim is not to expand the government's legal authority, but rather to ensure that we can obtain electronic information and evidence pursuant to the statutory 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. 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.

Counterintelligence

The nation faces a rising threat, both traditional and asymmetric, from hostile foreign intelligence services and their proxies. 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. They do so through 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. Foreign intelligence services and other State-directed actors continue to employ increasingly creative and 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 an insider violates the law and betrays the Nation's trust by leaking classified information, sometimes mixed with disinformation, to manipulate the public and advance a personal agenda.

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.

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 are constantly updating our intelligence apparatus to improve our ability to use, collect, and share intelligence, which will increase our understanding and allow us to defeat our adversaries. We cannot be content to work only the matters directly in front of us; intelligence allows us look beyond the horizon to identify the emerging threats we will face at home and abroad, and determine how those threats may be connected.

To that end, we gather intelligence, consistent with our legal authorities, to help us better understand and prioritize identified threats, to reveal the gaps in what we know about these threats, and to fill those gaps with new information. 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. Categorizing threats in this way allows us 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.

Integrating intelligence and operations is a part of the broader intelligence transformation the FBI has undertaken in the last decade to improve our assessment and mitigation of threats. Over the past few years, we have taken several steps to realize this integration. First, we established an Intelligence Branch within the FBI, headed by an Executive Assistant Director who is responsible for 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. As a result, they are better prepared to integrate their skillsets in their assignments. 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.

Cyber

Virtually every national security and criminal threat the FBI faces is either 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 also seek to strike our critical infrastructure and to harm our economy.

As the Committee is well aware, the frequency and effects 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 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. Cyber threats are also becoming increasingly difficult to investigate. For instance, 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 myriad 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.

Criminal

Public Corruption

Public corruption is one of the FBI's top criminal priorities. The threat—which involves the corruption of local, State, and Federally elected, appointed, or contracted officials—strikes at the heart of government, eroding public confidence and undermining the strength of our democracy. It affects how well U.S. borders are secured and neighborhoods are protected, how verdicts are handed down in court, and how well public infrastructure such as schools and roads are built. The FBI is uniquely situated to address this threat, with our ability to conduct

undercover operations, perform electronic surveillance, and run complex cases. However, partnerships are critical and we work closely with Federal, State, local, and tribal authorities in pursuing these cases.

One key focus is border corruption. The Federal government protects 7,000 miles of U.S. land border and 95,000 miles of shoreline. Every day, more than a million visitors enter the country through one of the 328 official Ports of Entry along the Mexican and Canadian borders, as well as through seaports and international airports. Any corruption at the border enables a wide range of illegal activities along these borders, potentially placing the entire nation at risk by letting drugs, guns, money, and weapons of mass destruction slip into the country, along with criminals, terrorists, and spies. FBI-led Border Corruption Task Forces are the cornerstone of our efforts to root out this kind of corruption. Located in nearly two dozen cities along our borders, these task forces consist of representatives from: the FBI; the Department of Homeland Security Office of Inspector General; Customs and Border Protection Office of Professional Responsibility; Transportation Security Administration; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms, and Explosives; U.S. Immigration and Customs Enforcement-Office of Professional Responsibility; and State and local law enforcement.

Civil Rights

The FBI remains dedicated to protecting the cherished freedoms of all Americans. This includes aggressively investigating and working to prevent hate crime, "color of law" abuses by public officials, human trafficking, and violations of freedom of access to clinic entrances and houses of worship—the four priorities of our civil rights program. We also support the work and cases of our local and State partners, as needed.

The investigation of hate crimes is the number one priority within the FBI's civil rights program due to the devastating effect these types of crimes can have not just on the victims and their families, but also on entire communities. A hate crime is a criminal offense against a person or property motivated in whole or in part by the individual's bias against a race, religion, disability, ethnic/national origin, sexual orientation, gender, or gender identity. While the First Amendment to the Constitution allows for the free expression of both offensive and hateful speech, this protection does not extend to criminal acts, even those done to express an idea or belief. The First Amendment also does not protect someone who issues a true threat to inflict physical harm on individuals or groups, or who intentionally solicits others to commit unlawful acts of violence on his or her behalf. The FBI investigated over 100 hate crime cases last year and remains dedicated to investigating these types of crimes. Additionally, the FBI proactively works to detect and deter future incidents through law enforcement training, public outreach, and partnerships with community groups.

Furthermore, we are focused on working with our State and local partners to collectively do a better job of tracking and reporting hate crime and "color of law" violations to fully understand what is happening in our communities and how to stop it. Our ability to address

significant national issues, such as the use of force and officer-involved shootings and jurisdictional increases in violent crime, depends on fuller statistical understanding of the underlying facts and circumstances. Some jurisdictions fail to report hate crime statistics, while others claim there are no hate crimes in their community—a fact that would be welcome, if true. We are dedicated to working vigorously with our State and local counterparts in every jurisdiction to better track and report hate crimes, in an accurate, timely, and publicly transparent manner.

Human Trafficking

Human trafficking is a modern form of slavery and a crime that the FBI is actively addressing. The majority of human trafficking victims recovered during FBI investigations are United States citizens, but traffickers are opportunists who will exploit any victim with a vulnerability. Victims of human trafficking are subjected to forced labor or sex trafficking, and the FBI diligently investigates both forms of human trafficking.

The FBI takes a victim-centered, trauma-sensitive approach to investigating these cases and strives to ensure the needs of the victims are fully addressed at all stages. To accomplish this, the FBI works in conjunction with other law enforcement agencies and victim specialists on the local, State, Tribal, and Federal levels, as well as a variety of vetted non-governmental organizations. Even after the arrest and conviction of human traffickers, the FBI often continues to work with these partner agencies and organizations to assist victims in moving beyond their exploitation.

The FBI addresses the human trafficking threat largely by working collaboratively with Federal, State, Tribal, and local law enforcement partners in working group and task force environments. The FBI funds 17 task forces dedicated to inter-agency cooperation to combat sex trafficking and labor trafficking. The task forces work cohesively to investigate cases, share valuable intelligence, and coordinate effective responses and prosecutions. The FBI also participates in DOJ-funded multi-disciplinary task forces. The FBI developed a Labor Trafficking Initiative to strengthen field office efforts to proactively identify forced labor targets.

Health Care Fraud

We have witnessed an increase in health care fraud in recent years, including Medicare/Medicaid fraud, pharmaceutical fraud, and illegal medical billing practices. Health care spending currently makes up about 18 percent of our nation's total economy. This large sum presents an attractive target for criminals. Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, and every taxpayer who funds Medicare is a victim. Schemes can also cause actual patient harm, including subjecting patients to unnecessary treatment or providing substandard services and supplies. As health care spending continues to rise, the FBI will use

every tool we have to ensure our health care dollars are used appropriately and not to line the pockets of criminals.

The FBI currently has 2,799 pending health care fraud investigations. Over 70 percent of these investigations involve government-sponsored health care programs, including Medicare, Medicaid, and TriCare, as well as other U.S. government-funded programs. As part of our collaboration efforts, the FBI maintains investigative and intelligence sharing partnerships with government agencies such as the Drug Enforcement Administration and other Department of Justice components, the Department of Health and Human Services, the Food and Drug Administration, State Medicaid Fraud Control Units, and other State, local, and tribal agencies. On the private side, the FBI conducts significant information sharing and coordination efforts with private insurance partners, such as the National Health Care Anti-Fraud Association, the National Insurance Crime Bureau, and private insurance investigative units. The FBI is also actively involved in the Healthcare Fraud Prevention Partnership, an effort to exchange facts and information between the public and private sectors in order to reduce the prevalence of health care fraud.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Today's gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit their illegal activities to single jurisdictions or communities. The FBI uses its institutional abilities to leverage cross-programmatic expertise to target gangs and violent crime, which is vital to the fight against violent crime in big cities and small towns across the nation. Every day, FBI special agents work in partnership with State, local, and tribal officers and deputies on joint task forces and individual investigations.

FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces—focus on identifying and targeting major groups operating as criminal enterprises. Much of the FBI's criminal intelligence is derived from our State, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

By way of example, the FBI has dedicated tremendous resources to combat the threat of violence posed by MS-13. The atypical nature of this gang has required a multi-pronged approach—we work through our task forces here in the U.S. while simultaneously gathering intelligence and aiding our international law enforcement partners. We do this through the FBI's Transnational Anti-Gang Task Forces ("TAGs"). Established in El Salvador in 2007 through the

FBI's National Gang Task Force, Legal Attaché ("Legat") San Salvador, and the United States Department of State, each TAG is a fully operational unit responsible for the investigation of MS-13 operating in the northern triangle of Central America and threatening the United States. This program combines the expertise, resources, and jurisdiction of participating agencies involved in investigating and countering transnational criminal gang activity in the United States and Central America. There are now TAGs in El Salvador, Guatemala, and Honduras. Through these combined efforts, the FBI has achieved substantial success in countering the MS-13 threat across the United States and Central America.

Despite these efforts, we still have work to do. The latest Uniform Crime Reporting statistics gathered from the *Crime in the United States, 2016*, show the number of violent crimes in the nation increased by 4.1 percent compared with the 2015 estimate, and this year we are also seeing an uptick of homicides in some cities. Compared with 2015, the number of estimated homicides in the nation rose 8.6 percent in 2016.

Transnational Organized Crime

More than a decade ago, the image of organized crime was of hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or States, but organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion dollar schemes from start to finish. These criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identity theft, human trafficking, and other illegal activities. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and Federal, State, local, tribal, and international partners. The FBI continues to share intelligence about criminal groups with our partners and to combine resources and expertise to gain a full understanding of each group.

Opioids

Large amounts of high quality, low cost heroin and illicit fentanyl are contributing to record numbers of overdose deaths and life-threatening addictions nationwide. Transnational Criminal Organizations ("TCOs") are also introducing synthetic opioids to the US market, including fentanyl and fentanyl analogs. To address this evolving threat, we are taking a multi-faceted approach and establishing many initiatives and units across our criminal program.

One response to this threat is our Prescription Drug Initiative ("PDI"). The PDI was established in 2016 in response to the substantial and increasing threat associated with prescription drug diversion, and in particular, the staggering national increase in opioid related deaths. The objective of the PDI is to identify and target criminal enterprises and other groups engaged in prescription drug schemes; identify and prosecute, where appropriate, organizations with improper corporate policies related to prescription drugs; and identify and prosecute, where

appropriate, organizations with improper prescribing and dispensing practices. The PDI prioritizes investigations which target "gatekeeper" positions, to include medical professionals and pharmacies that divert opioids outside the scope of their medical practice and/or distribute these medications with no legitimate medical purpose. Since its inception, the PDI has resulted in the conviction of numerous medical professionals and secured significant Federal prison sentences to include life terms for physicians who cause harm or death to the patients entrusted to their care. In August of 2017, PDI resources were enlisted to support the Attorney General's Opioid Fraud and Abuse Detection Unit in 12 judicial districts significantly affected by the opioid crisis.

The Hi-Tech Organized Crime Unit ("HTOCU") is another response to the growing opioid epidemic. This unit focuses on the trafficking of opioids via the Internet, specifically the Darknet. HTOCU is leading a proactive effort to increase awareness, train personnel, and provide guidance to FBI field offices on how to successfully address this threat. As a result, numerous investigations and operations have been initiated and several online vendors who are facilitating the trafficking of opioids via the Internet, to include Fentanyl, have been disrupted.

Beyond these two programs, the FBI has dedicated additional resources to address this expansive threat. We have more than doubled our number of Transnational Organized Crime Task Forces, expanded the Organized Crime Drug Enforcement Task Force ("OCDETF") Airport Initiative to focus on insider threats partnering with TCO actors, and created and led the Fentanyl Safety Working Group at FBI Headquarters, which has led to a new program to protect field agents and support employees with personal protective equipment ("PPE") and opioid antagonists (i.e. naloxone) from the threat of fentanyl exposure. The FBI participated, along with other Federal partners, in the creation of the Heroin Availability Reduction Plan ("HARP"), takes part in monthly HARP meetings hosted by the Office of National Drug Control Policy ("ONDCP"), and continues to provide training to our international law enforcement partners on successful identification, seizure, and neutralization of clandestine heroin/fentanyl laboratories.

Crimes Against Children

The FBI remains vigilant in its efforts to eradicate predators from our communities and to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA analysis, trace evidence, impression evidence, and digital forensics. Through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world, and these outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate both parents and children about the dangers posed by predators and to recover missing and endangered children. To this end, the FBI funds or participates in a variety of endeavors, including our Child Abduction Rapid Deployment Teams, Innocence Lost National Initiative, Innocent Images National Initiative, annual Operation Cross Country, Victim Services Division, 78 Child Exploitation Task Forces, 63 International

Violent Crimes Against Children Task Force Members, and numerous community outreach programs.

Operation Cross Country, a nationwide law enforcement action focusing on underage victims of sex trafficking, completed its eleventh iteration during the second week of October and recovered 84 minors. Over 400 agencies across 55 FBI Field Offices were instrumental in recovering child victims of all backgrounds and arresting sex traffickers, including sex customers. More than 100 victim specialists, in coordination with local law enforcement victim advocates and non-governmental organizations, provided services to child and adult victims.

Indian Country

There are 567 federally recognized Indian tribes in the United States, with the FBI and the Bureau of Indian Affairs having concurrent jurisdiction for felony-level crimes on over 200 reservations. According to the 2010 Census, there are nearly five million people living on over 56 million acres of Indian reservations and other tribal lands. Criminal jurisdiction in these areas of our country is a complex maze of tribal, State, Federal, or concurrent jurisdiction.

The FBI's Indian Country program currently has 135 special agents in 34 FBI field offices primarily assigned to Indian Country crime matters. The number of agents, the vast territory, and the high frequency of violent crime handled by these agents makes their responsibility extremely challenging. The FBI has 16 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country, and we continue to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska Natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country matters involve death investigations, physical and/or sexual assault of a child, or aggravated assaults. At any given time, approximately 30 percent of the FBI's Indian Country investigations are based on allegations of sexual abuse of a child.

The FBI continues to work with tribes through the Tribal Law and Order Act of 2010 to help tribal governments better address unique public safety challenges and disproportionately high rates of violence and victimization in many tribal communities. The act encourages the hiring of additional law enforcement officers for Native American lands, enhances tribal authority to prosecute and punish criminals, and provides the Bureau of Indian Affairs and tribal police officers with greater access to law enforcement databases.

FBI Laboratory

The FBI Laboratory is one of the largest and most comprehensive forensic laboratories in the world. Operating out of a state-of-the-art facility in Quantico, Virginia, laboratory personnel travel the world on assignment, using science and technology to protect the nation and support law enforcement, intelligence, military, and forensic science partners. The Lab's many services include providing expert testimony, mapping crime scenes, and conducting forensic exams of physical and hazardous evidence. Lab personnel possess expertise in many areas of forensics supporting law enforcement and intelligence purposes, including explosives, trace evidence, documents, chemistry, cryptography, DNA, facial reconstruction, fingerprints, firearms, and WMD.

One example of the Lab's key services and programs is the Combined DNA Index System ("CODIS"), software the FBI develops and administers, which allows 200 law enforcement laboratories throughout the United States to compare over 16 million DNA profiles. In the last twenty years, CODIS has aided nearly 400,000 investigations, while maintaining its sterling reputation and the confidence of the American public.

The Terrorist Explosives Device Analytical Center ("TEDAC") is another example. Formally established in 2004, TEDAC serves as the single interagency organization that receives, fully analyzes, and exploits all priority terrorist improvised explosive devices ("IEDs"). TEDAC coordinates the efforts of the entire government, including law enforcement, intelligence, and military entities, to gather and share intelligence about IEDs. These efforts help disarm and disrupt IEDs, link them to their makers, and prevent future attacks. For example, Laboratory Division personnel recently testified in New York in the successful prosecution of Muhanad Mahmoud Al Farekh after linking him to a vehicle-borne improvised explosive device prepared for an attack on the US military base in Afghanistan. Although originally focused on devices from Iraq and Afghanistan, TEDAC now receives and analyzes devices from all over the world.

The National Institute of Justice ("NIJ") and the FBI have continued their partnership aimed at addressing a critical and complex issue in our nation's criminal justice system: untested sexual assault kits ("SAKs"). The FBI Laboratory has been a leader in developing best practices for DNA testing. By serving as a single laboratory for SAKs submitted by law enforcement agencies and public forensic laboratories nationwide, the FBI was able to offer proven methods for improving the collection and processing of quality DNA evidence. This information was published this summer in NIJ's document "National Best Practices for Sexual Assault Kits: A Multidisciplinary Approach."

Additionally, the Laboratory Division maintains a capability to provide forensic support for significant shooting investigations. The Laboratory Shooting Reconstruction Team provides support to FBI field offices by bringing together expertise from various Laboratory components to provide enhanced technical support to document complex shooting crime scenes. Services are

scene and situation dependent and may include mapping of the shooting scene in two or three dimensions, scene documentation through photography, including aerial and oblique imagery, 360 degree photography and videography, trajectory reconstruction, and the analysis of gunshot residue and shot patterns. Significant investigations supported by this team include the shootings at the Inland Regional Center in San Bernardino, California; the Pulse Night Club in Orlando, Florida; the Route 91 Harvest Music Festival in Las Vegas, Nevada; and the shooting of 12 police officers during a protest against police shootings in Dallas, Texas.

Conclusion

The strength of any organization is its people. The threats we face as a nation are as great and diverse as they have ever been, and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States and the men and women of the Bureau work hard to meet and exceed those expectations, every day. I want to thank them for their dedication and their service.

Chairman Goodlatte, Ranking Member Nadler, and members of the Committee, thank you again for this opportunity to discuss the FBI's programs and priorities. Mr. Chairman, we are grateful for the support that you and this Committee have provided to the FBI. We would not be in the position we are today without it. Your support of our workforce, our technology, and our infrastructure make a difference every day at FBI offices in the United States and around the world, and we thank you for that support. I look forward to answering any questions you may have.