Department of Justice

STATEMENT OF

CHRISTOPHER WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

JULY 23, 2019

STATEMENT OF
CHRISTOPHER WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. SENATE

AT A HEARING ENTITLED
"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED
JULY 23, 2019

Good morning Chairman Graham, Ranking Member Feinstein, and members of the Committee.

Thank you for inviting me to appear before you today. I'm honored to be here, representing the men and women of the FBI. Our people – nearly 37,000 of them – are the heart of the Bureau. I'm proud of their service and their commitment to our mission. Every day, they tackle their jobs with perseverance, professionalism, and integrity.

In the past two years, I have had the chance to visit all 56 Field Offices. I've visited the home states of every member of this Committee, talking with state and local law enforcement partners and people in your communities about the issues that matter most to them. I'm grateful for their support and insights as we work together to keep 325 million American people safe, and to help make our communities stronger.

Today's FBI is a national security and law enforcement organization that uses, collects, and shares intelligence in everything we do. Each FBI employee understands that, to defeat the key threats facing our nation, we must constantly strive to be more efficient and more effective. 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.

National Security

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. However, the threat posed by terrorism — both international terrorism ("IT") and domestic terrorism ("DT") — 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 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 Qaeda 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 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 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 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 y, 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. However, continued counterterrorism pressure has degraded the group, and in the near term al Qaeda is more likely to focus on supporting small-scale, readily achievable attacks against U.S. and allied interests in the Afghanistan/Pakistan region. Simultaneously, over the last year, propaganda from al Qaeda leaders seeks to inspire individuals to conduct their own attacks in the 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. We anticipate law enforcement, racial minorities, and the U.S. government will continue to be significant targets for many domestic violent extremists.

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 include covert actions by foreign governments to influence U.S. 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, 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 include targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft; criminal efforts to suppress voting and provide illegal campaign financing; 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 our ideas — 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 and to harm our economy.

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.

Criminal Threats

We face many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent crime and public corruption. Criminal organizations — domestic and international — and individual criminal activity represent a significant threat to our security and safety in communities across the Nation. A key tenet of protecting the Nation from those who wish to do us harm is the National Instant Criminal Background Check System, or NICS. The goal of NICS is to ensure that guns do not fall into the wrong hands, and also to ensure the timely transfer of firearms to eligible gun buyers. Mandated by the Brady Handgun Violence Prevention Act of 1993 and launched by the FBI on November 30, 1998, NICS is used by Federal Firearms Licensees ("FFLs") to instantly determine whether a prospective buyer is eligible to purchase firearms. NICS receives information from tens of thousands of FFLs and checks to ensure that applicants do not have a criminal record or are not otherwise prohibited and therefore ineligible to purchase a firearm. In the first complete month of operation in 1998, a total of 892,840 firearm background checks were processed; in 2018, almost 2.2 million checks were processed per month.

While most checks are completed by electronic searches of the NICS database within minutes, a small number of checks require examiners to review records and resolve missing or incomplete information before an application can be approved or rejected. Ensuring the timely processing of these inquiries is important to ensure law abiding citizens can exercise their right to purchase a firearm and to protect communities from prohibited and therefore ineligible individuals attempting to acquire a firearm. The FBI is currently processing a record number of checks, over 26 million were processed in 2018.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Many of today's gangs are sophisticated and well organized and use violence to control neighborhoods, and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. These gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is able to work across such lines, 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 federal, 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 — focus on identifying and targeting major groups operating as criminal enterprises. Much of the FBI 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.

We are committed to working with our federal, State, local, and Tribal partners in a coordinated effort to reduce crime in the United States.

Transnational Organized Crime ("TOC") and Opioids

More than a decade ago, organized crime was characterized by 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. Modern-day 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, modern criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, drug trafficking, identity theft, human trafficking, money laundering, alien smuggling, public corruption, weapons trafficking, extortion, kidnapping, and other illegal activities. TOC networks exploit legitimate institutions for critical financial and business services that enable the storage or transfer of illicit proceeds. Preventing and combating transnational organized crime demands a concentrated effort by the FBI and federal, State, local, Tribal, and international partners.

While the FBI continues to share intelligence about criminal groups with our partners and combines resources and expertise to gain a full understanding of each group, the threat of transnational crime remains a significant and growing threat to national and international security with implications for public safety, public health, democratic institutions and economic stability across the globe.

Illicit drug trafficking continues to be a growing threat. Large amounts of high-quality, low cost heroin and illicit fentanyl are contributing to record numbers of overdose deaths and life-threatening addictions nationwide. The accessibility and convenience of the drug trade online contributes to the opioid epidemic in the United States. Transnational criminal organizations ("TCOs") are introducing synthetic opioids to the U.S. market, including fentanyl and fentanyl analogues. To address this evolving threat, we are taking a multi-faceted approach and establishing many initiatives and units across our criminal program.

In January 2018, the Office of the Deputy Attorney General directed the FBI and other federal law enforcement partners to develop a strategic plan to disrupt and dismantle the Darknet illicit marketplaces facilitating the distribution of fentanyl and other opioids. As a result, the FBI established the Joint Criminal Opioid Darknet Enforcement ("J-CODE") Initiative, which brings together agents, analysts, and professional staff with expertise in drugs, gangs, health care fraud, and more, with federal, State, and local law enforcement partners from across the U.S. Government. The J-CODE team has developed a comprehensive, multi-pronged criminal enterprise strategy to target the trafficking of fentanyl and other opioids on the Darknet and Clearnet. This strategy focuses on identifying and infiltrating the marketplace administrative team, analyzing financial information, locating and exploiting marketplace infrastructure, targeting vendors and buyers, and enabling field office success in

the investigation and prosecution of these marketplaces. 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.

The FBI is also addressing this threat through the 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.

Beyond these two programs, the FBI has dedicated additional resources to address this expansive threat. We have more than doubled the 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 implementation 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 and Human Trafficking

It is unthinkable, but every year, thousands of children become victims of crimes — whether it is through kidnappings, violent attacks, sexual abuse, human trafficking or online predators. The FBI is uniquely positioned to provide a rapid, proactive, and comprehensive response; identify, locate, and recover child victims; and strengthen relationships between the FBI and federal, State, local, Tribal, and international law enforcement partners to identify, prioritize, investigate, and deter individuals and criminal networks from exploiting children.

The FBI has several programs in place to arrest child predators and to recover missing and endangered children. To this end, the FBI funds or participates in a variety of endeavors, including our Innocence Lost National Initiative, Innocent Images National Initiative, Operation Cross Country, Child Abduction Rapid Deployment Teams, Victim Services, 80

Child Exploitation Task Forces, 53 International Violent Crimes Against Children Task Force Officers, as well as numerous community outreach programs to educate parents and children about safety measures they can follow.

Currently, there are at least 30 child pornography sites operating openly and notoriously on the Dark Net, including the Tor network. Some of these child pornography sites are exclusively dedicated to the sexual abuse of infants and toddlers. The sites often expand rapidly, with one site obtaining 150,000 new members within its first seven weeks of operation. The FBI combats this pernicious crime problem through investigations such as *Operation Pacifier*, which targeted the administrators and users of a highly-sophisticated, Tor-based global enterprise dedicated to the sexual exploitation of children. This multi-year operation has led to the arrest of over 348 individuals based in the United States, the prosecution of 25 American child pornography producers and 51 American hands-on abusers, the rescue or identification of 55 American children, the arrest of 548 international individuals, and the identification or rescue of 296 children abroad.

Child Abduction Rapid Deployment Teams are ready response teams 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.

In addition to programs to combat child exploitation, the FBI also focuses efforts to stop human trafficking — a modern form of slavery. 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 is working hard with its partners to combat both forms.

The FBI works collaboratively with law enforcement partners to investigate and arrest human traffickers through Human Trafficking Task Forces nationwide. We take a victim-centered, trauma-informed approach to investigating these cases and strive to ensure the needs of 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 with a variety of vetted non-governmental organizations. Even after the arrest and conviction of human traffickers, the FBI often continues to work with partner agencies and organizations to assist victims in moving beyond their exploitation.

Earlier this year, the FBI announced the results of an 11-day effort by the Violent Crimes Against Children/Human Trafficking Program and the Metro Atlanta Child Exploitation ("MATCH") Task Force. The effort, leading up to Super Bowl LIII, was collaborated with over 25 local, State, and federal law enforcement agencies and District Attorney's Offices, along with seven non-government organizations. From January 23, 2019 to

February 2, 2019, the operation's goal was to raise awareness about sex trafficking by proactively addressing that threat during the Super Bowl and events leading up to the Super Bowl. This event led to 169 arrests, including 26 traffickers and 34 individuals attempting to engage in sex acts with minors; nine juvenile sex trafficking victims recovered (the youngest was 14 years of age); and nine adult human trafficking victims identified. Trafficking is not just a problem during large-scale events — it is a 365 day-a-year problem in communities all across the country.

The FBI commends the Committee's dedication to these efforts and appreciates the resources provided to combat these horrific acts.

Key Cross-Cutting Capabilities and Capacities

I would like to briefly highlight some key cross-cutting capabilities and capacities that are critical to our efforts in each of the threat and crime problems described.

Operational and Information Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts. The FBI is using technology to improve the way we collect, analyze, and share information. We have seen significant improvement in capabilities over the past decade; but keeping pace with technology remains a key concern for the future.

The volume of data collected in the course of investigations continues to rapidly expand. In the case of the 2017 Las Vegas shooting, the FBI recovered one petabyte of data. Insufficient network bandwidth and tools necessitated the need for 260 FBI personnel to work over 10 days to manually review 21,500 hours of video footage. These bandwidth and data challenges are not limited to major cases or large offices. It is not uncommon for FBI investigations to generate more than one terabyte of data per day, an amount that could normally take two days to transit FBI networks at current bandwidth levels. As a result, the FBI has made dedicated efforts to upgrade and transform its information technology platforms to meet the demands of current and future investigations. To keep pace in an era where investigations and analysis will increasingly be conducted at the petabyte scale, the FBI needs to build networks that can move bulk data, modernize investigative data analysis, and reduce reliance on stand-alone, ad-hoc systems.

A key tenet of this transformation is the integration of Data Analysts ("DA") in field offices nationwide. A DA is able to clean, standardize, enrich, and visualize data using computer programming and statistical techniques to provide products to the investigative team to further investigative matters. They are able to create code tailored to intelligence and investigative requirements to triage and prioritize vast amounts of data received by investigative teams, enabling efficient follow-on analysis; convert thousands of location points contained in cellphone call and data records into a usable format for follow-on network and

geospatial analysis; and combine dozens of differently formatted files into an easy-to-read, consolidated format, free of duplicate and inconsistent information. In FY 2018, the FBI piloted the DA program by sending analysts to several FBI Field Offices. The DAs helped those offices address several of their most critical data challenges, and were able to solve volume, velocity, and geospatial data issues. In one instance, investigators wanted to determine what businesses a credit card skimming subject visited to place money orders. The DA converted hundreds of pages of call detail records to a machine readable format, plotted location points onto a map to show the subject's location over time, and calculated the proximity to vendors where fraudulent activity may have occurred. The DA's mapping product not only provided pattern of life information (leading to the discovery of new investigative leads), but also saved investigators days, if not weeks. The FY 2020 Request expands the 2018 pilot program by requesting an additional 25 Data Analysts to deploy to the most critical field offices. The FBI will continue to monitor and measure the success of this program.

The FBI Laboratory is one of the largest and most comprehensive forensic laboratories in the world. Operating out of a 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 counterterrorism and forensic research.

The Terrorist Explosives Device Analytical Center ("TEDAC") is a key 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 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 a U.S. military base in Afghanistan. Although originally focused on devices from Iraq and Afghanistan, TEDAC now receives and analyzes devices from all over the world.

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.

FBI Special Agents and Intelligence Analysts need the best technological tools available to be responsive to the advanced and evolving threats that face our nation. Enterprise information technology must be designed so that it provides information to operational employees rather than forcing employees to conform to the tools available. IT equipment must be reliable and accessible, thus decreasing the time between information collection and dissemination.

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 Graham, Ranking Member Feinstein, and members of the Committee, thank you again for this opportunity to discuss the FBI's programs and priorities. We are grateful for the leadership that you and this Committee have provided to the FBI. Your support for 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.