CHRISTOPHER WRAY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
STATEMENT BEFORE THE SENATE APPROPRIATIONS COMMITTEE,
SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE
AND RELATED AGENCIES
WASHINGTON, D.C.

MAY 16, 2018

Good afternoon Chairman Moran, Ranking Member Shaheen, and members of the Subcommittee.

Thank you for allowing me to appear before you today. The Federal Bureau of Investigation (FBI) especially thanks this Committee for its support of the men and women of the FBI in the Fiscal Year (FY) 2018 Appropriation. As the Committee is aware, FBI personnel are the lifeforce of the organization – they work tirelessly to combat some of the most complex and serious national security threats and crime problems challenging the Nation's intelligence and law enforcement communities. The funding you provided is imperative in allowing the FBI to retain these precious assets – our personnel – as well as address these considerable threats.

Today, I appear before you on behalf of these men and women who tackle these threats and challenges every day. I am extremely proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our Nation. On their behalf, I would like to express my appreciation for the support you have given them in the past, ask for your continued support in the future, and pledge to be the best possible stewards of the resources you provide.

I would like to begin by providing a brief overview of the FBI's FY 2019 budget request, and then follow with a short discussion of key threats and challenges that we face, both as a Nation and as an organization.

FY 2019 Budget Request Overview

The FY 2019 budget request proposes a total of $8.92 billion in direct budget authority to carry out the FBI's national security, criminal law enforcement, and criminal justice services missions. The request includes a total of $8.87 billion for Salaries and Expenses, which will support 34,694 positions (12,927 Special Agents, 3,055 Intelligence Analysts, and 18,712 professional staff), and $51.9 million for Construction.

As a result of this budget being formulated before the Bipartisan Budget Act of 2018, it was built utilizing the prior year enacted level as a starting point. Accordingly, this request sustains prior

year personnel and operational funding, but provides no discrete program enhancements. The request also includes a cancellation of $148 million from Criminal Justice Information Services (CJIS) automation fund available surcharge balances.

When compared against the FY 2018 Omnibus enacted level, the FY 2019 request level represents a total decrease of $476 million, including a $318 million reduction in the FBI's Construction account funding for one-time projects, and a $158 million reduction to the Salaries and Expenses account.

Key Threats and Challenges

This Committee has provided critical resources for the FBI to become what it is today – a threat-focused, intelligence-driven organization. Our Nation continues to face a multitude of serious and evolving threats ranging from homegrown violent extremists to hostile foreign intelligence services and operatives; from sophisticated cyber-based attacks to internet facilitated sexual exploitation of children; from violent gangs and criminal organizations to public corruption and corporate fraud. Keeping pace with these threats is a significant challenge for the FBI. As an organization, we must be able to stay current with constantly changing and new technologies that make our jobs both easier and harder. Our adversaries – terrorists, foreign intelligence services, and criminals – take advantage of modern technology, including the Internet and social media, to facilitate illegal activities, recruit followers, encourage terrorist attacks and other illicit actions, and to disperse information on building improvised explosive devices and other means to attack the U.S. The breadth of these threats and challenges are as complex as any time in our history. And the consequences of not responding to and countering threats and challenges have never been greater.

The support of this Committee in helping the FBI to do its part in facing and thwarting these threats and challenges is greatly appreciated. That support is allowing us to establish strong capabilities and capacities for assessing threats, sharing intelligence, leveraging key technologies, and – in some respects, most importantly – hiring some of the best to serve as Special Agents, Intelligence Analysts, and professional staff. We have built and are continuously enhancing a workforce that possesses the skills and knowledge to deal with the complex threats and challenges we face today – and tomorrow. We are building a leadership cadre that views change and transformation as a positive tool for keeping the FBI focused on the key threats facing our Nation.

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 continue to 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 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. 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 feel empowered to act out in support; (2) those who are enabled to act after gaining inspiration from extremist propaganda and communicating with members of foreign terrorist organizations who provide guidance on operational planning or targets; and (3) those who are directed by members of foreign terrorist organizations to commit specific, directed acts in support of the group's ideology or cause. Prospective terrorists can fall into any of the above categories or span the spectrum, 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, federal, 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, in a manner consistent with the First Amendment, 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. 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. 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 Qaeda maintains its desire for large-scale attacks; however, continued counterterrorist 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, however, and especially over the last year, propaganda from al Qaeda 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 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.

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.

A particular focus of our counterintelligence efforts is 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 another company or country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations.

To combat this threat, the FBI has undertaken several initiatives. We developed and deployed the Hybrid Threat Center (HTC) to support Department of Commerce Entity List investigations. The HTC is the first of its kind in the FBI; it has been well-received in the U.S. Intelligence Community and the private sector.

Over the past year, we have strengthened collaboration, coordination, and interaction between our Counterintelligence and Cyber Divisions in an effort to more effectively identify, pursue, and defeat hostile intelligence services 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 available on our public website, which has been shown thousands of times to raise awareness and generate referrals from the private sector.

Cyber Threats

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek 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 strike our critical infrastructure and to harm our economy.

As the committee is well aware, the frequency and impact of cyber-attacks on our Nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow. We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as other technically sophisticated attacks. 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 fight the full range of cyber threats. And 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 are 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— thereby 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.

Going Dark

The rapid pace of advances in mobile and other communication technologies continue to present a significant challenge to conducting court-ordered electronic surveillance of criminals and terrorists. 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 use 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.

Where they can, 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 is often not sufficient to meet the rigorous constitutional burden to prove crimes beyond a reasonable doubt. Likewise, 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 life cycle or as a consequence of disclosure through legal proceedings.

We respect the right of Americans 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 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 already has provided to us to keep America safe. 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. 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 neutral judge 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 effects of the Going Dark challenge on both public safety and the rule of law, and with the academic community and technologists to encourage their voluntary cooperation to work with us on developing technical solutions to this problem.

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 don't fall into the wrong hands, and also ensures 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 buy firearms. NICS receives information from tens of thousands of FFLs and checks to ensure that applicants do not have a criminal record or aren't 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 2017, approximately 2.1 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, averaging over 2.3 million a month during the first three months of 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 SafeTrails—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.

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 although preliminary data for 2017 shows that violent crime overall is leveling off and murder may be on the decline, there are still jurisdictions that are struggling. We also still have far to go before crime rates are back to the levels in 2014 and 2015. We are committed to working with our federal, state, local, and tribal partners toward that end.

Transnational Organized Crime

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, 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.

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.

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 U.S. 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 Dark Net. 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 also 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, annual 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.

The FBI committed significant resources to Operation Pacifier, which targeted the administrators and users of "Playpen" – a members-only website on the Tor anonymity network run by a highly-sophisticated, global enterprise dedicated to the sexual exploitation of children. To date, in the United States this operation has led to the arrest of over 348 individuals, the prosecution of 25 child pornography producers and 51 hands-on abusers, and the rescue or identification of 55 children. This operation has also yielded the arrest of 548 individuals abroad, and the identification or rescue of 296 children abroad. These successes only underscore how much work remains to address child exploitation on the Dark Net.

Another such program is Operation Cross Country. This nationwide law enforcement action focuses on underage victims of sex trafficking, completed its 11th iteration during the second week of October and recovered 84 minors. Over 400 agencies partnering with 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.

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.

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. We are using technology to improve the way we collect, analyze, and share information. We have seen significant improvement in capabilities and capacities over the past decade; but keeping pace with technology remains a key concern for the future.

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, digital forensics and weapons of mass destruction (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 20 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 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. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps. We then try to fill those gaps and continue to learn as much as we can about the threats we are addressing and those we may need to address. 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 develop a threat prioritization ranking for each of the FBI's 56 field offices. By creating this ranking, we strive to actively pursue our highest threats where they are occurring. This gives us a better assessment of what the dangers are, what's being done about them, and what we should spend time and valuable resources on.

A key challenge inhibiting our ability to address current and future threats is the lack of a headquarters facility that fully fosters collaboration, intelligence sharing, and is dynamic, enabling Special Agents, Intelligence Analyst, and other Professional Staff to combat evolving threats as they arise. The current J. Edgar Hoover building is incompatible with what the United States expects of the FBI. Our goal is to build a consolidated, secure, resilient intelligence community-worthy facility. But even more than that, what we need is a facility capable of meeting the increased demands of the Nation's premier Intelligence and Law Enforcement organization for the future of the FBI. This building will address the way we will work for the next 50 or more years.

Being expected to respond to a wide range of complex and ever-changing threats and crime problems is not new to the FBI. Our success in meeting these challenges is, however, directly tied to the resources provided to the FBI. The resources the Committee provides each year are critical for the FBI's ability to address existing and emerging national security and criminal threats.

Chairman Moran, Ranking Member Shaheen, and members of the Subcommittee, I would like to close by thanking you for this opportunity to discuss the FBI's FY 2019 budget request and the key threats and challenges that we are facing, both as a nation and as an organization. We are grateful for the leadership that you and this subcommittee have provided to the FBI. We would not possess the capabilities and capacities to deal with these threats and challenges today without your support. Your willingness to invest in and support our workforce and our physical and technical infrastructure allow the men and women of the FBI to make a difference every day in communities large and small throughout our nation and around the world. We thank you for that support.

I look forward to answering any questions you may have.