

**COMMERCE, JUSTICE, SCIENCE, AND RE-
LATED AGENCIES APPROPRIATIONS FOR
FISCAL YEAR 2019**

WEDNESDAY, MAY 16, 2018

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 2:31 p.m., in room SD-138, Dirksen Senate Office Building, Hon. Jerry Moran (Chairman) presiding.

Present: Senators Moran, Murkowski, Collins, Boozman, Capito, Lankford, Shaheen, Leahy, Feinstein, Coons, and Van Hollen.

FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF HON. CHRISTOPHER A. WRAY, DIRECTOR

OPENING STATEMENT OF SENATOR JERRY MORAN

Senator MORAN. As soon as I can see you, Director, I will call the Subcommittee on Commerce, Justice, and Science, and Related Agencies to come to order.

We have logistical issues today, in which there are votes called at 3 o'clock. I think there are two votes. Our hearing was intended and will be a two-part set of hearings, this one in public, and then we will convene to the Sensitive Compartmented Information Facility (SCIF) in the Visitors Center in the United States Capitol for a more classified briefing. We intend to do that.

Senator Shaheen and I have generally agreed to forgo our opening statements. I will hold Members, Senator Feinstein is the only one here to hear this, but I will do everything I can, including with Senator Leahy, to restrict everyone to their 5 minutes, and I will use the gavel to accomplish that.

I will also attempt to call the hearing to reconvene in the SCIF following the second vote of a two-vote series, so we will try to get started as early as we can there. In that setting, we will work hard to give everybody an opportunity to pursue things that maybe they did not get to pursue here.

Let me just say, as my opening statement, Director, it is an honor to have you here in front of us. It has been a pleasure to get to know you. I express my gratitude to you and the people who work at the FBI and other agencies related to our national security and combating crime and terrorism. I am very grateful for their service to our Nation and the efforts that are so often successful

in protecting us from lots of harm in the lives of American citizens, so I am grateful for the service of you and the FBI that you serve. Senator Shaheen is forgoing her opening statement. Director Wray, we would call upon you for your testimony.

SUMMARY STATEMENT OF HON. CHRISTOPHER A. WRAY

Director WRAY. Thank you, Mr. Chairman, Ranking Member Moran, and Members of the subcommittee. I am honored to be here representing the men and women of the FBI. Our employees, as the subcommittee knows, are spread across more than 350 locations all around the country, in 90 offices around the world, and in 34 headquarters divisions.

What strikes me the most in coming back to working with the organization every day after a hiatus is the people—people tackling their jobs with strength and honesty and professionalism; people committed to doing the right thing in the right way; people fiercely committed to protecting the American people from terrorists and criminals and spies; and people following the facts independently no matter where they lead and no matter who likes it.

Our people, nearly 37,000 of them, are the heart of the FBI. Through their sense of duty and commitment, our employees embody our core values and our motto of fidelity, bravery, and integrity.

So I want to thank you for the funding you have provided us in 2018. Without it, we would not be able to do all that great work.

In the interest of the subcommittee's time, I have shortened what I was going to say here at the beginning and included a lot more details about our budget request in my written statement for the record. I am also happy to address questions about our budget here today, in addition to questions about threats we face and the FBI's critical capabilities.

This subcommittee has always been tremendously supportive of the Bureau and giving us the resources that we need. I look forward to discussing how we can maintain our capabilities through the resource investments provided by the fiscal year 2018 budget, as enacted, and how we can build on that momentum going forward. In particular, I hope to be able to discuss the threats we face on the FBI's critical capabilities. We have a lot of things on our plate, and some of the key priorities, obviously, are counterterrorism, counterintelligence, cyber threats, transnational organized crime, violent crime, the opioid epidemic, and child predators. That is just at the top of the list.

The threats are of grave importance to our security. We want the American people to be able to focus on just living their lives while we focus on keeping them safe. I am incredibly proud of the FBI's work, but we cannot afford to be complacent. We have to keep pace with technology in all those areas that I listed and seek out new, innovative solutions to the problems we face. Because if we do not do that, our adversaries are not going to wait around on us—and we must keep pace with them.

We cannot do any of that without your support and without the resources that you provide. As always, we are committed to being good stewards of those funds.

Thank you for having me here today, and I look forward to answering your questions.
[The statement follows:]

PREPARED STATEMENT OF HON. CHRISTOPHER A. WRAY

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 2018 appropriation. As the Committee is aware, FBI personnel are the life force 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 fiscal year 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.

FISCAL YEAR 2019 BUDGET REQUEST OVERVIEW

The fiscal year 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 fiscal year 2018 Omnibus enacted level, the fiscal year 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 United States. 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 ac-

cess 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 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, healthcare, 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 3 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 foren-

sic 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 organi-

zation 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 fiscal year 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.

Senator MORAN. Thank you, Director. I will begin with my round of questioning. I will try to do so very briefly as well.

USA GYMNASTICS

I had intended to ask much more budget-oriented questions before I got to this one, but I do want to highlight the importance to me in an effort that our subcommittee in Commerce—I Chair a subcommittee in Commerce that is responsible for Olympic and amateur sports through the Ted Stevens Olympic and Amateur Sports Act. Senator Feinstein from California has been hugely engaged in this issue. But our subcommittee is looking at the issue of the perspective of what happened to gymnasts, in particular, but Olympian sports figures as a result of sexual abuse.

In our investigation, we have collected thousands of documents and have had two hearings. One of the things, Director, that I wanted to ask you, let me read this so I get it correct: There are current and former athletes who have come forward with accusations of abuse by individuals associated with their sport, and Michigan State's response to claims of sexual abuse indicate that those indications were such that the FBI had been notified. As you would know, Dr. Larry Nassar has been convicted and is serving prison time. But the follow-up to that has been that the various entities who received reports of this abuse had an indication from the FBI not to say anything and that the FBI had been notified.

I know that you have commenced an investigation, an internal investigation, of what transpired, but the answers to these questions are important to us as we pursue additional hearings in the near future.

So, Director, I would appreciate anything that you can tell me about whether or not reports of abuse of athletes were made to the FBI, and if the FBI would have encouraged or insisted that the people making those reports say nothing to anyone else.

Director WRAY. Mr. Chairman, as we have discussed, obviously, I think what happened to those women is horrific, and I am gratified that Dr. Nassar is being held accountable and will be spending the rest of his life in prison.

I first learned that there were questions about the FBI's response to allegations when during the 2015–2016 period when those things were happening. I learned of the allegations in February

when the newspapers started raising the issue. I immediately commissioned our Inspection Division to do a deep dive after-action report to look at what was done, what was not done, what lessons we can learn and how we can make sure that we are doing things appropriately.

That review is ongoing, so I do not have anything to report on right now. But I am very much looking forward to that and am committed to taking appropriate steps once I hear what they find.

Senator MORAN. I look forward to following that report's completion, having a full understanding of what transpired, because it will have consequences for others involved that we are investigating.

Let me just ask a general question. It is related to the one that we just discussed.

CONGRESSIONAL OVERSIGHT

I am of the view that the appropriations process needs to work. We need to march 12 appropriations bills across the Senate floor, across the House floor, and be considered by a President. Obviously, the appropriations process is about spending money and priorities, which we look forward to hearing more from you about, but it is also about oversight. I want this subcommittee to be in a position in which we pursue whether or not taxpayer dollars are wisely spent.

I would just ask you, at this point, tell me your view about congressional oversight. What do you expect to be the relationship between our subcommittee and other congressional committees in regard to the FBI? And what is its responsibility to Congress?

Director WRAY. Mr. Chairman, this is an important topic to me. We respect very much the importance of traditional congressional oversight. We welcome the tough questions, given our responsibilities, and we are committed to being as responsive as we can to appropriate questions and requests. Of course, we are also committed to being faithful to our oath to protect the American people and uphold the Constitution.

All of us in the intelligence community understand that to include, as it always has, protection of sources and methods. I will tell you that, as anybody in the intelligence community knows, human sources, in particular, who have put themselves at great risk to work with us and with our foreign partners have to be able to trust that we are going to protect their identities and, in many cases, their lives and the lives of their families. The day that we cannot protect human sources is the day the American people start becoming less safe.

Senator MORAN. Thank you, Director.

Let me now turn to the Ranking Member, Senator Shaheen.

Senator SHAHEEN. Thank you, Mr. Chairman.

USA GYMNASTICS

It is nice to have you here, Director Wray. I want to follow up on Senator Moran's question about the investigation into USA Gymnastics and Larry Nassar, and applaud his efforts as head of the Commerce subcommittee that is looking into this matter.

You may not know the answer. If you do not, I hope you will see if you can find out and include that information in what is provided to this subcommittee. When FBI agents interviewed individuals who had alleged abuse by Nassar, do you know if there were victim specialists or, in the case of minors, child adolescent forensic interviewers, there for those interviews?

Director WRAY. Senator, I do not know the answer to that question. I do know that our Office of Victim Assistance, as we call it, is an incredibly important function for us, in particular to deal with victims exactly like these folks. They are stretched very, very thin. But the reason we call them Office of Victim Assistance is because they are designed to help victims. It is not just to make them possible witnesses.

Senator SHAHEEN. I hope your investigation will examine that matter and make sure if the appropriate people were not present, that it will reflect that, so that we have that information in the future.

Also, do you commit to sharing the summary results of that internal review with this subcommittee?

Director WRAY. I would be happy to make sure that we are providing the subcommittee all appropriate information about that review. At the moment, I do not know yet what they are going to find, of course, but this is an important topic to me. There is nothing more important, no category of victims more important, than the most vulnerable populations, which includes our kids.

Senator SHAHEEN. Absolutely. I think the question is not just if Larry Nassar will be held accountable, but also any other participants in USA Gymnastics or the U.S. Olympic Committee who knew what was going on. We need to hold those individuals accountable, too.

ELECTION SECURITY

When you and I spoke on the phone, and I appreciated your call, we talked about the elections coming up. The intelligence community has said there are reasons to believe the interference we saw in the 2016 election by the Russians will be occurring in 2018 or there will be an effort to interfere again in 2018. Can you talk about what the FBI is doing to secure our election systems?

Director WRAY. I think in particular—we work very closely with the Department of Homeland Security and others. Our role, in particular, is focused on trying to identify the threat, investigate the threat, pursue and disrupt the threat. One of the first things I did after getting sworn in as Director was create a Foreign Influence Task Force, which brings together our Counterintelligence Division, our Cyber Division, our Criminal Division, and even our Counterterrorism Division, believe it or not, with the idea of having a single, consolidated, coordinated effort that makes this issue a priority. And we work with our colleagues at DHS. We work with our foreign partners, because, of course, they have concerns about efforts to interfere or influence, I should say, their elections.

So we are actively working with a particular focus on 2018 and then, ultimately, 2020.

Senator SHAHEEN. I am really pleased to hear that, and I look forward to hearing more details about that in our closed session,

because I think this is not a partisan issue. This is an issue about a foreign government's efforts to undermine our system of government and, ultimately, our way of life in America. So, whatever the FBI can do to address that issue I think is very important.

BLACK CUBE

On May 6, "The New Yorker" ran what I thought was a very troubling story about an Israeli private-intelligence firm called "Black Cube". The firm, apparently, is accused of performing an undercover campaign to discredit Obama administration officials who were proponents of the 2015 Iran nuclear deal. The firm has also been accused of being used by Harvey Weinstein to gather intelligence on his victims in order to stop the publication of sexual misconduct allegations against him.

What is the FBI's role in investigating this kind of organization?

Director WRAY. Senator, of course, I cannot comment on or even confirm the existence of any specific investigation. But what I can tell you is that we look at these things through two lenses. There is both a criminal lens and a counterintelligence lens.

On the counterintelligence lens, any time a firm that might be working on behalf of a foreign power, for example, we would want to be approaching whether or not there are counterintelligence implications from that end of it. Likewise, on the criminal side, we would be looking at any kind of firm that might be engaged in any violation of Federal criminal law. There are many of those, as you can imagine.

Senator SHAHEEN. Thank you. My time is up. I apologize for leaving to go to another hearing, but I look forward to seeing you in the closed session.

Senator MORAN. Senator Shaheen, thank you for your questioning in regard to the athletes. I appreciate your leadership in this regard. I know how seriously you take it.

Senator Lankford is next recognized. We are going to hold you to the time limit as best I can.

Senator LANKFORD. I will take it from there. Thank you, Mr. Chairman.

DOCUMENT REQUESTS

Director, good to see you again. Over the past 6 months, there have been numerous document requests back and forth with the FBI. The FBI has hired additional contractors to be able to expedite some of that process.

Can you give me an update on requests from the House and the Senate for any documents that we have requested either from the House or Senate to be able to have access to, redacted or unredacted? What is the status of those at this point?

Director WRAY. Senator, as you alluded to; we actually have been dealing with quite a number of requests, some of them almost unprecedented in their volume from a number of different committees. We have, in the case of one committee, for example, doubled the number of people working on it basically around the clock, full-time, to over 50 people.

So we are chugging away, making progress. A lot of the redactions, depending on the particular committee requesting, have

to do with things like grand jury secrecy, where we legally have an implication or, as I referenced with the Chairman, protection of human sources and methods, or, in some cases, ongoing investigations.

So we are trying our best to be responsive, but we are also trying to be responsible.

Senator LANKFORD. Sure. So do you have any deadlines when they will be—all documents that are currently in request—I am sure there is always another request coming.

Director WRAY. Well, it is rolling. I do not have numbers for you here right now, with that level of specificity in this hearing. But I can tell you that every week we are cranking out documents and people are coming over to spaces that we have set aside for the Hill to review documents. So it is an ongoing process of thousands of documents being produced.

FBI AND ATF PROCESSES ALIGNMENT

Senator LANKFORD. Sure. Let me switch over. The Department of Justice and I started a conversation about 6 years ago about trying to align the processes of FBI and ATF, because they are both doing investigations, but their processes are very different. I know you do not oversee ATF, but I have continued to be able to raise the Department of Justice to be able to take a look at those two processes and make sure they are good and consistent. Quite frankly, I think the FBI has a very good process to be able to go through how you conduct investigations, how you gather evidence, what you do. There may be some things to be able to learn from ATF.

Do you know if there has been outreach from DOJ yet to FBI to be able to look at processes at FBI, to try to lay that comparison with ATF?

Director WRAY. Senator, I do not know specifically about that. I will tell you that we work daily with ATF. They are great partners. As you say, while I am sure there are things they can learn from us, there are definitely things we can learn from them, too, so we are in constant contact at all levels.

Senator LANKFORD. Great. We will continue to follow up on that.

BACKGROUND CHECK

The background checks have been a constant issue about trying to raise the number of background checks and the speed of those. The FBI is obviously very involved in helping with that process.

Can you help us understand better what can be done better not only to up the speed but to give your agents more time to be able to work on transnational criminal organizations, crimes against children, and so many other things that you do rather than so much time on the background checks? Is there a better way to do it?

Director WRAY. I think we are all frustrated at the pace. We have to be thorough. We have to be careful.

I think one of the challenges that we deal with is that, when we are running searches, we are fundamentally, at the FBI, a field-deployed organization, so it is not just that there could be one place centrally at headquarters that would have all that information.

Nominees could probably be faster in getting us paperwork because that is where we start. But there are a lot of different ways in which lots of us have to do more. We have looked at things, and we do do things like use retired agents who sometimes come back as contractors, because they have that some of that judgment and experience. All of that requires resources, but that is another way we are trying—

Senator LANKFORD. If there are ways that we can help on that, we are very interested in being able to get that from you. Obviously, we do not want to take a lot of time from your agents' time with other projects they have. This is very important as well, to be able to do background checks with great speed, but it also takes a tremendous amount of time.

TRANSNATIONAL ORGANIZED CRIME

Let me switch over to transnational criminal organizations to try to see the focus you have had and the cooperation with U.S. attorneys at this point, because that requires a tremendous amount of coordination with all areas DHS, all areas, obviously, of the FBI, U.S. attorneys.

What are you seeing at this point in the transnational criminal organizations?

Director WRAY. I think transnational criminal organizations are maybe one of the least talked about but yet most pervasive threats we have to deal with. We see it not just in the obvious in terms of drug trafficking and all kinds of violent crime, but even the things that might not be as obvious to the American people. Of course, they are involved in human trafficking. We have seen reporting about them relying on intellectual property theft of all kinds of things to raise revenue.

So pretty much any violation that the subcommittee can think about, transnational criminal organizations are in them. So we are seeing that more and more.

I think one of the strengths that the FBI brings to the table, over the course of its entire 110-year history, is a focus on organized crime, dismantling enterprises, going after not just the people but taking apart their infrastructure, taking away their money, all of that. So it is something that I think we are going to have to put even more focus on and kind of capture also the global cross-border dynamics.

So at the end of the day, I think it comes down to technology and the cross-border dimension to it. Those are the trends that I would most cite to you on that.

Senator LANKFORD. We want you to keep your eye on the ball on that and will be glad to be able to help. Let us know what you need.

Director WRAY. Thank you.

Senator MORAN. The Vice Chairman of the full committee is recognized, Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman.

Director Wray, thank you for being here today. As you know, I began my career in law enforcement. I watch the FBI and others, and I hope you will take back to the bureau my thanks to the men

and women who are working every day to uphold the integrity and independence of the FBI. That is important to all of us.

I have a number of questions for you.

I will note for the record the President's budget request reduces overall FBI funding by 5 percent. They request no funding for the new FBI headquarters. They request a rescission of another \$148 million in salaries and expenses. I am going to give you a question for the record of how that will impact the ability of the FBI to do its job.

Frankly, I am concerned with this administration—I would be concerned with any administration, but this one especially with the relentless, politicized attacks on our Nation's law enforcement institutions, because I think that could affect their independence. There is a unifying theme to it. They attack anybody who has investigated Russia's interference in our democracy.

RUSSIA INVESTIGATION

The President has called your bureau "a disgrace". The Chair of the House Intelligence Committee suggested you should be impeached, which goes beyond balderdash. It is one of the dumbest statements I have heard any Member of Congress of either party ever say, and I have heard a few in both parties.

You have been the Director of the FBI since August. Do you believe the men and women of the FBI working on the Russia investigation are driven by anything other than a duty to the rule of law and to ensuring that anyone who attacked our democracy in 2016 is held accountable?

Director WRAY. Senator, I can only speak to what I have seen since I have been on the job, but the agents that I have worked with since being on the job have inspired me every day in terms of their professionalism, their integrity, their courage, and their commitment to doing the right thing in the right way, which I think is the key.

Senator LEAHY. You said at your confirmation hearing that the Russia investigation was not a "witch hunt". You have been there as the FBI Director for 10 months. You are far more immersed in the details of the FBI. Is that still your opinion?

Director WRAY. Yes.

ZTE

Senator LEAHY. Thank you. You also recently testified that you are "deeply concerned" about allowing the Chinese cell phone company ZTE to operate within the United States because of the potential for espionage.

The company also violated sanctions and sold technology to North Korea and Iran, and our Commerce Department has brought charges against them. But the President announced on Twitter this week that he has "instructed" his Commerce Department to get ZTE "back in business, fast", so those Chinese jobs are not lost.

If the President allows ZTE further access to our market and to American technology, could this place both our telecommunications networks and Americans' private data at-risk?

Director WRAY. Senator, the questions about the Commerce Department's settlements, its remedies, and penalties, I would defer to the Commerce Department.

Senator LEAHY. I understand.

Director WRAY. But what I can tell you is that we at the FBI remain deeply concerned that any company beholden to foreign governments that do not share our values are not companies that we want to be gaining positions of power inside our telecommunications network.

That gives them the capacity to maliciously modify or steal information. That gives them the capacity to conduct undetected espionage. That gives them the capacity to exert pressure or control.

So all of those are things that we were concerned about with any company that, as I say, is beholden to a foreign government.

Senator LEAHY. But this company, is there pretty well a consensus among our intelligence people, the FBI included, that they do pose a threat or a potential threat to us?

Director WRAY. Again, I want to be careful in this setting in commenting on a specific company, but I remain of the view that I have articulated before about companies of this sort and the capacity that giving them access to our telecommunications network provides.

Senator LEAHY. You had earlier testified specifically on ZTE.

Director WRAY. In response to a question about that company, I provided an answer almost identical to what I just did here. My view has not changed since that earlier testimony.

Senator LEAHY. I share your concern about ZTE. I was concerned that, 72 hours after the Chinese Government pumped a half billion dollars into a theme park in Indonesia that had Donald Trump's name on it, he said we should put those people back to work.

But that is probably just coincidence, Mr. Chairman.

Senator MORAN. Senator Leahy, thank you.

Senator COLLINS.

Senator COLLINS. Thank you, Mr. Chairman.

Welcome, Director, and thank you for your leadership.

HOMEgrown EXTREMISTS

A major challenge for the FBI is homegrown extremists in every State in the Nation who have been inspired by ISIS or Al Qaeda or similar groups, and radicalized no longer by traveling to training camps but via the Internet through videos or private chat rooms or other means.

How is the FBI countering that threat? It seems to be very difficult to identify these individuals.

Director WRAY. Senator, you are exactly right. You put your finger on what I would call sort of our highest counterterrorism priority at the moment. We have about 1,000 investigations into exactly the kind of people you are describing, covering all 50 States as I am sitting here right now. That is not even counting the Al Qaeda investigations, the traditional ISIS investigations, or the domestic terrorism investigations, but just the group you are talking about.

What makes it so hard is that there are not many dots to connect with some of these people. They pick soft targets. They use easy-

to-use weapons, IEDs, cars, knives, guns. And they can make decisions on the spur of the moment.

We are trying to get better at looking for red flags as to when people who are getting radicalized make that switch into potentially mobilizing. A lot of that is outreach to the community, and partnership with our State and local law enforcement who know those communities better, but it is hard.

It is something that I compare notes with my foreign counterparts on a lot, and they have the same challenge. All of our closest allies have the same issue.

NO FLY, NO BUY

Senator COLLINS. I introduced a bill that we refer to as the No Fly, No Buy legislation. What it says is that, if you are listed on the Government's terrorist watch list—and I am not talking about the very broad one; I am talking about the no-fly list—where you are considered to be so dangerous that we do not allow you to board an airplane—now, obviously, a lot of the people on this list are not Americans, but there is a small subset that is. Our bipartisan bill says that you should not be able to purchase a firearm if you are on that list.

It has robust due-process provisions, so you can challenge the denial of the firearm purchase in Federal court. If you win, your attorney fees are reimbursed to you.

Do you think that is a good policy for us?

Director WRAY. I certainly, like you, want to make sure that we are keeping guns out of the wrong hands. I think I would have to look hard at the legislation itself to have a better sense of not just legally, which I would consult with the Department on, but operationally what it would mean. So I would be happy to take a closer look at the bill.

Senator COLLINS. Thank you. That would be helpful.

CYBERSECURITY

Finally, how is the FBI responding to the growing cybersecurity threat from both state and nonstate actors, particularly with regard to our critical infrastructure, such as the electrical grid?

Director WRAY. We are doing a number of things, both on the enforcement and investigations side but also on the outreach and communication side. We have cyber task forces in every field office. We have a 24/7 Cyber Watch, kind of like our Strategic Information and Operations Center (SIOC) on that terrorism side. We have a number of things like that that help lead the investigation.

Then on the outreach side, we try to communicate with the critical infrastructure private sector and give them threat information so that they can better prepare. We are trying to be more forward-leaning all the time. I talk about this when I meet with the private sector—how we can better get them timely, actionable, relevant information, so that they can take steps to harden their infrastructure.

Of course, we work very closely with the Department of Homeland Security on that as well. It is a mission that we try to tackle together, each of us with our own respective responsibilities.

Senator COLLINS. Thank you. I think that communication with the private sector in both directions is absolutely critical, so that you can share threat information, malicious software signatures.

There was a DOD study with defense contractors that did that, and people were amazed to find that they did not have the same information. So I think that can be valuable.

Thank you, Mr. Chairman.

Senator MORAN. Thank you, Senator Collins.

The Senator from California, Senator Feinstein.

USA GYMNASTICS

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Director, I wanted to ask you one question on the Larry Nassar case. Last year, the Senate Judiciary Committee held a hearing on abuse within Olympic sports. Two survivors testified about being abused by Dr. Nassar. He is taken care of.

What is troubling to me is, last week, a gold medal Olympian came in and spoke to the Chairman of the Judiciary Committee and myself to say that she reported abuse to a specific local office, which I will give you privately, that she had suffered abuse, and nothing was done about it. She tried for a year with the FBI in that office and then gave up.

So the question I have is, has the FBI been instructed to take these complaints seriously and promptly respond to women making them? Because I am really concerned about it. These are all young women, and they deserve an investigation.

Director WRAY. Senator, I share your concern. My heart goes out to the victims of Dr. Nassar.

As I think I might have mentioned earlier in the hearing, once I heard that there were questions about the stuff that had happened in 2015 and 2016, I commissioned an internal deep-dive by our Inspection Division to do a full after-action report to figure out what we did in all the different offices that might have been involved, what we did not do, and what lessons we can learn.

I have not gotten the results of that yet. It is still ongoing. But I intend to make sure that, if there were mistakes made, we learn from those mistakes.

Senator FEINSTEIN. Thank you. And will you share that study with us?

Director WRAY. I would be happy to share the appropriate information with the subcommittee.

NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS)

Senator FEINSTEIN. Another question, following the murders of the nine churchgoers at Emmanuel AME in South Carolina in 2015, the FBI admitted it did not properly obtain information regarding the gunman's drug arrest record, which should have prohibited him from buying a handgun. The FBI apparently had not completed its review within 3 days, so the dealer was legally permitted to complete the sale to the gunman. As we know, nine people died as a result.

Are there instances where State records or other records cannot be physically obtained within a 3-day delay period by the FBI?

Director WRAY. I do not know if I can speak for all 50 States on that. I have actually gone out to the National Instant Criminal Background Check System (NICS) in West Virginia and sat there and listened in on the earpieces, so I can actually hear what our folks do and what it is like to actually take one of these calls. We do try very hard to turn them around as quickly as we can, but we need to be right.

I will tell you, you might be interested to know that, in the first 3 months of this year, we have had a record number of NICS checks.

Senator FEINSTEIN. A record number of?

Director WRAY. NICS checks per month each of those months.

So we are doing a ton of work. That can always get better. I do know that some States, the way they keep the records in terms of what they reflect as a disposition, for example, on a prior arrest does not necessarily fit as well in our system, so it takes more work to kind of drill down and understand. It gets really obscure, but it depends on which subsection of the code as to whether it is actually a prohibitor or not and things like that. So we are always getting better.

Senator FEINSTEIN. Do you think the 3-day provision should be eliminated?

Director WRAY. I would have to look at the implications of that.

Senator FEINSTEIN. Okay, would you look and just give us a recommendation one way or another.

Director WRAY. I would be happy to tell you what I think the operational impact of that would be.

Senator FEINSTEIN. Good.

You say in your written testimony that, "Domestic violent extremist movements collectively pose a steady threat of violence and economic harm to the United States." That is a quote.

HATE CRIMES/DOMESTIC TERRORISM

In 2015, the FBI reported that there were 5,850 incidents of hate crimes, and specific offenses against Muslims grew 67 percent from 2014.

Given this tremendous increase, what is the FBI doing to increase its investigative resources related to hate crimes?

Director WRAY. Well, we have dedicated units that focus on civil rights offenses, including hate crimes. Also, we find with some frequency that hate crimes and domestic terrorism—and I think the reference that I was making that you are referring to was intended to speak about domestic terrorism, which may or may not, depending on the instance, be the same thing as a hate crime. So our Joint Terrorism Task Forces (JTTFs) make that a principal area of focus.

And we have, ironically, about the same number of domestic terrorism investigations, which is about a thousand, as we do home-grown violent extremists. And that covers the waterfront, though, all the way from white supremacist investigations all the way to anarchist investigations and pretty much everything in between.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Senator MORAN. Thank you, Senator Feinstein.

The Senator from Arkansas, Senator Boozman.

Senator, I would tell you, before you arrived, we are close on time. I would encourage you, if you are going to ask questions, to stay within the 5 minutes. We have Senator Coons, Senator Van Hollen—

Senator BOOZMAN. I will do whatever you tell me to do today.

[Laughter.]

Senator MORAN. The Senator is recognized.

Senator BOOZMAN. Thank you very much.

Thank you, Director, for being here. We really do appreciate your hard work. I know Senator Collins has already asked about it, so I am not going to ask again about cybersecurity, and how important that is. I think all the subcommittee shares that thought. Anything we can do to help you in that regard, we will.

CHILD EXPLOITATION

One of the issues in your testimony that you touched on was child exploitation. As you know, the Department of Homeland Security also was very interested in that. Can you talk about your abilities to work together? Are you working together?

Director WRAY. We do work together on those issues. We have Task Forces specifically focused on child exploitation, child pornography, and different kinds of sexual crimes focused on children. I think Homeland Security makes a great partner on that. Both of us rely very heavily on State and local law enforcement, because it requires that, too.

There is also a role, I think, for victim services because these are unusually difficult cases, just given the nature of the victim population. We have something called Innocence Lost, which is an initiative of ours. It is intelligence-driven. It is kind of focused on trying to make sure we have the maximum impact. And, of course, the role of cyber, as you mentioned, in your other topic becomes inextricably intertwined with that.

NICS

Senator BOOZMAN. I also would like to ask a little bit about NICS in the sense that we have Arkansans that, for one reason or another, maybe they have similar names, have wound up in a situation where they have been denied and then want to appeal. The backlog on that is great right now.

Can you talk to us a little bit about how you are trying to address that?

Director WRAY. Certainly, the resource constraints that we have at NICS are significant. As I mentioned, we had a record number of checks the first 3 months of this year. We try very hard to make sure that we do not have delays within the time period allowed.

In my experience, the vast majority of calls can be dealt with in the same phone call. As I mentioned, I wanted to kind of see what it is like to be out there in person, so I actually went out to West Virginia and sat in the call center, put earpieces on, and actually listened to an operator doing a few of these.

Some of them can be greenlighted right there on the call. Some of them can be denied right there on the call. A lot of them require

a little more work, which I think usually can be done within the time period allowed.

Senator BOOZMAN. Very good. That would be a nice place to go visit. Maybe we will get an opportunity to do that.

I yield back, in an effort to accommodate my colleagues.

Senator COLLINS [presiding]. Thank you. It is great being Chairman, however briefly.

Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Senator Collins.

Director Wray, thanks for being here, and thank you to the men and women of the FBI for helping protect our country.

FBI HEADQUARTERS

You say in your testimony that it is important that the FBI have a new headquarters. You talked about the current condition of the J. Edgar Hoover Building. I must say, for those of us who have been following this process for many years, we have gotten whiplash when it comes to the FBI building.

Let me read to you from a 2016 prospectus from the GSA that was put together after years of congressional input, GSA input, FBI input, congressional support. It said that the current building cannot be redeveloped to provide the necessary space and consolidate the FBI headquarter components or to meet the agency's physical security requirements. They go on to say very specifically that they looked at the idea of redeveloping the FBI building at its current site and said that it was not capable of meeting the security setback requirements.

As you know, other major security facilities—CIA, NSA, Cyber Command—they are on campus settings with these large setbacks. Don't those large setbacks provide extra, enhanced security to the people who work in those places?

Director WRAY. Senator, obviously, security is extremely important not just to our folks but to me since I would have to work in the building. The proposal that we have on the table right now would allow us to get to a Level V security, much like our partners, say Scotland Yard and various others around the world who function like us.

So we are comfortable that putting in place a new building—not renovating the old one but a brand-new building in that space—allows us to be able to kind of do both things, which is to take advantage of the location that we need but at the same time provide the security—

Senator VAN HOLLEN. Mr. Director, with all respect, you are going to have to convince me anyway that the reasons why the FBI and the GSA have rejected their earlier assessment that developing at the current site regardless of the configuration would provide adequate security. That is the same reason we have the CIA on a campus, that we have NSA on a campus.

I have to go on, but it just does not compute that larger setbacks do not provide more security. So the question would be what kind of security you are willing to give up.

ZTE

Here is what I want to ask you. I want to go back to Senator Leahy's questions about ZTE and your earlier testimony before the Senate Intelligence Committee. My understanding is you maintain the same assessment today as before. Is that right?

Director WRAY. Yes.

Senator VAN HOLLEN. Just to put it bluntly, what was President Trump thinking when he tweeted out what he did about putting ZTE back in business?

Director WRAY. Senator, I cannot speak to what anybody else was thinking. I am not really a Twitter guy. What I will tell you is that we take very seriously our obligation to protect our national security, so we look at it through the lens of what kind of capacity providing a company that is beholden to another government that may not share our values—

Senator VAN HOLLEN. So the fact that you do not know what he was thinking tells me he did not consult with you or anyone at the FBI before he sent that out, did he?

Director WRAY. Well, I would not get into our discussions, but I would just say that my assessment—

Senator VAN HOLLEN. Well, no, that is not a discussion. No, come on. I mean, did the President reach out to you and the FBI before he sent out his tweet on ZTE? That is an important question.

I mean, if he did, it suggests that he took into account or rejected your advice. I am just asking if the President asked you—

Director WRAY. I am not aware of any discussion of that sort.

Senator VAN HOLLEN. Do you know if ZTE has accessed U.S. trade secrets and provided them to the Chinese Government?

Director WRAY. I am sorry, could you repeat that?

Senator VAN HOLLEN. Do you know if there is any evidence that ZTE has accessed stolen U.S. trade secrets and provided them to the government?

Director WRAY. Senator, I am not sure there is anything I could say on that topic in this setting.

ELECTION SECURITY

Senator VAN HOLLEN. All right. My last questions really relate to what Senator Shaheen said. Your colleagues in the law enforcement community have indicated they expect that the Russians will interfere in the midterm 2018 elections, very much like they did before. When you testified back in February, you indicated that the President had not directed you or the FBI to take any additional actions to confront Russian interference.

My question is, have you heard from the President on that issue since February? Has he directed you and the FBI to enhance your operations in preparation for midterm elections?

Director WRAY. Senator, we did in fact, as I think the White House has reported, meet. A group of us—me, the Secretary of Homeland Security, the Director of National Intelligence, the Attorney General, and others did meet with the President not that long ago where he emphasized the importance of protecting our election from foreign interference.

Senator VAN HOLLEN. All right, I am going to send you a written question regarding legislation Senator Rubio and I have introduced called the DETER Act.

Thank you.

Director WRAY. Thank you, Senator.

Senator MORAN [presiding]. Thank you, Senator Van Hollen.

The Senator from West Virginia, Senator Capito.

Senator CAPITO. Thank you, Mr. Chairman.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Thank you, Mr. Director, for being here. I caught, just as I walked in, you talked about your visit to West Virginia. So that was going to be my first question, to talk about the CJIS Division in Clarksburg, the great work that they are doing there not just on the NICS system but on a lot of the background checks, et cetera.

I did not know if there was anything you wanted to add about that facility. Obviously, we are very proud of it in West Virginia and the good work that is done there.

Director WRAY. I would be happy to. I really enjoyed my visit out there. All I had really covered so far about what is out there are questions about NICS.

Of course, as you know, there is a lot of very important work being done out there, everything from the National Crime Information Center (NCIC) to the Uniform Crime Reporting Program (UCR), and the National Incident-Based Reporting System (NIBRS) that does the crime reporting statistics. There is just a lot out there, our Public Access Line that takes calls from the public.

It is a thriving facility with great people working really, really hard. I was very impressed by what I saw out there.

Senator CAPITO. Thank you. We are certainly glad you are there.

FBI HEADQUARTERS

I would say, my cohort from Maryland, in talking about the headquarters, I understand that part of the plan on the headquarters remaining toward the downtown area would be to move some of the existing employees or maybe functions to other places, one of which was Clarksburg, I believe.

Did you have any thoughts on that?

Director WRAY. For about a decade now, the FBI has been working on plans to move various functions and headcount out of the National Capital region, including not just Clarksburg but Huntsville; Pocatello, Idaho, on the IT side; and even Quantico.

The new headquarters proposal that we have would significantly expand the number of people who would be in the headquarters building here. So it is a combination of things.

TASK FORCE OPERATIONS

Senator CAPITO. Okay. As you are aware, State and Federal authorities successfully executed a widescale takedown operation of the Peterson drug trafficking organization in Huntington, West Virginia, and Detroit as part of Operation Saigon Sunset. As a result, the officers apprehended 90 suspected drug suppliers and traf-

fickers; 167 grams of cocaine; 760 grams of heroin; 450 grams of fentanyl, which is enough to kill 250,000 individuals.

I just want to thank you and your department and the coordinating aspects of what you have done with the U.S. attorney's office. I understand every law enforcement officer that was in any part of that area was a part of that.

I just want to know, is this typical of what the FBI is doing around the country, in terms of being able to fortify those local resources to be able to catch these guys? Because, literally, they are killing our people.

Director WRAY. This is a huge priority for us. One of the things I have been trying very hard to do as Director is not spend all my time inside the beltway. I have been trying to get out. I am determined to try to get to all 56 of our Field Offices by the end of this year. I am making good headway.

Every office I go to, there is incredible work being done by the men and women of the FBI on some of the same kinds of issues you are talking about. It never fails to give me an extra spring in my step. We could not do it, though, without our partners. That is the important piece. It is not just the FBI. It is us with DEA, ATF, HSI, and State and local partners, in particular.

Key is that we have a lot of task force officers. We have about 500-and-something task forces, that is not even counting the Joint Terrorism Task Forces, and over 7,000 task force officers, which means officers from State and local law enforcement, for example.

Through the resources this committee provides us, we are paying their overtime, their use of vehicles, et cetera. Frankly, if you looked at the number of task force officers that we work with every day in all of our field offices, there are actually more task force officers than there are agents on task forces. So they are a huge part of it. It is very much a team effort. We are grateful for their support.

Senator CAPITO. I appreciate that. I think I stated earlier, we really could not do it without that leadership, without the expertise and technology and the intelligence and everything that comes along with the good men and women of the FBI. Thank you very much.

Director WRAY. And we could not do it without the subcommittee's support, frankly, because the threats, everywhere I go, somebody has some idea of something the FBI should do more of. I have not found very many people with good ideas of what the FBI should do less of yet. So we are stretched thin, but we are working hard with our partners.

Senator CAPITO. We will be there to support you. Thank you.

Director WRAY. Thank you.

Senator MORAN. The Senator from Delaware, Senator Coons.

Senator COONS. Thank you, Chairman Moran.

Director Wray, it is good to be with you. I think we have known each other for about 25 years, and it is great to see you in this role, and I am grateful for what you and the terrific men and women of Federal law enforcement and, in particular, the FBI do week in and week out, their service, their devotion to the country, to the Constitution, and to the rule of law.

You are literally the Federal cops on the beat, as you were just discussing with the Senator from West Virginia. You play a key part in making sure that not just Federal law enforcement, but Federal, State, and local law enforcement is highly effective. And you keep all Americans safe regardless of their political leanings, their backgrounds, their race, their religion or creed.

When you took the oath last August, you took it to protect our Constitution, not to protect any individual or any party.

FBI EFFECTIVENESS

I have to say, I am deeply troubled by recent baseless attacks on the FBI. Would you agree that the effectiveness of the FBI really depends on citizens, on witnesses, on juries, on State and local law enforcement all being able to have trust in the FBI?

Director WRAY. Senator, the people you just listed off are great examples of the opinions that matter to me most and that matter to our people most. There are a lot of opinions out there about the FBI, just like there are about everybody in this room. But the opinions that matter the most are the opinions of juries when our agents take the stand; the opinions of magistrate judges when our agents bring them a search warrant; the opinions of our State and local partners, if they trust us to work with them; our private sector partners; our community partners; judges; as I mentioned before, victims and their families, do they trust us? Those are the opinions of people who know us through our work, and those are the opinions that matter to me and to our people.

Senator COONS. I hope that you do not find the opinions of some discouraging or dispiriting.

This is National Police Week. We are all in our Nation's Capital honoring the men and women of law enforcement across the country. But we have seen, I think tragically, a series of public statements by President Trump suggesting that the investigation into Russian interference in the 2016 election is "a witch hunt."

He literally said last month, "You look at the corruption at the top of the FBI, it's a disgrace."

Now, if this was just some stray comment, there is a wide range of opinions in our country, as you mentioned, we could dismiss it. But I am concerned it is beginning to have an impact.

There was a poll of 1,500 Americans released last week by the Economist that said 7 percent of Democrats, 25 percent of independents, and 61 percent of Republicans said the FBI is framing the President with the Department of Justice.

Let me repeat that: 61 percent of Republicans surveyed said the FBI and the Justice Department are framing the President of the United States.

That seems to me directly opposite the care, the diligence, the professionalism, the dedication to rule of law that I have known in the men and women who I know in the FBI, in our field office in Delaware and here, in my service in the Senate.

Director, can I just ask you, are the FBI and the Department of Justice in any way attempting to frame the President of the United States?

Director WRAY. Senator, the people that I work with every day, the people that I see every day inside the FBI, are committed to

doing the right thing in the right way with professionalism, integrity, objectivity, and courage. So while I recognize that there are, as I said, a lot of opinions out there, we do not focus on polls and surveys and studies. We focus on, as I said, the opinions of people who know us through our work.

What I find when I go out and talk to people in the field out on the frontlines, our partners, the judges, the prosecutors, the victims, the feedback I get uniformly is positive and supportive.

Senator COONS. Should you come to visit the field office in Wilmington, Delaware, I think you will get exactly that same feedback. The FBI is a highly valued part of our local law enforcement community and a great contributor.

There was a case just last month in Kansas where three men were convicted of plotting to blow up an apartment complex and mosque, and the FBI could disrupt this plot because an informant trusted the FBI. Jurors trusted the FBI, all the evidence it developed and brought forward, despite attacks on the FBI from the defense in that specific case.

So I will just conclude on this point by saying that I think trust in the FBI is absolutely essential to the rule of law in our country. I did not mean to berate you on the point. I just think we cannot go without commenting on the fact that there is, in my mind, a steady erosion in confidence, and there is a cause of it, and I truly hope that the men and women of the FBI know that they have strong bipartisan support here in Congress.

NICS

Let me ask you a last question. My home community of Wilmington, as I know you know, has faced an epidemic of gun violence in recent years. We have had a lot of assistance from Federal law enforcement. One of the things we are trying to do is to make sure that we keep guns out of the hands of persons prohibited. That is why I joined with Senator Toomey to introduce the NICS Denial Notification Act, which requires the Federal Government to notify State and local law enforcement when a person prohibited fails a background check.

Last year, the NICS section denied 104,000 firearm transactions where people who are prohibited by law attempted to buy.

Do you think it would be helpful for Federal law enforcement to notify State law enforcement when someone prohibited from owning a firearm attempts to purchase one?

Director WRAY. Senator, obviously, we, like you, want to make sure we are keeping guns out of the hands of the wrong people—those who are prohibited by law from possessing them. And NICS denials are a key tool in that.

I have not studied the bill that you are describing. We do feel very strongly about our need to work closely with State and local partners to share information. I would have to look at the operational impact of that. Obviously, there is always a balance. We all feel in today's world in law enforcement that we want more information, but we also get deluged with information. So we have to work through some of those issues.

I will say, on Wilmington, as you may know, the Task Force that we have had working there, I think there has been a 71 percent drop in gun crime in the last year.

Senator COONS. We are very hopeful. Summer is just getting started. We are hoping that trend will hold.

Director WRAY. We had an arrest just yesterday, actually, there on a kidnapping, murder charge related to one of the big gangs in Wilmington.

Senator COONS. You did. I will forward you the bill. Thank you for your indulgence.

Thank you very much for your service.

Senator MORAN. The Senator from Alaska, Senator Murkowski.

Senator MURKOWSKI. Thank you, Mr. Chairman. I will be brief, because I know we have a vote that has begun.

Director Wray, thank you for being here. Thank you for what you do. I want to just reassure that I join with the Senator from Delaware and the Senator from West Virginia, my support for the good work that the men the women of the FBI deal with every day.

I certainly have had my differences with the FBI over the years, particularly as it related to the handling of former Senator Stevens' investigation. I am still not satisfied that the agency properly investigated the whistleblower who called attention to the misconduct in the investigation and the prosecution. But I want to make very clear, I have not lost faith in the FBI as an institution.

I had an opportunity just a few months back to meet with the special agent in charge in Anchorage and his senior team to convey the point directly, to get an update from all of them, to look them all in the eyeball and just let them know that we have great faith in the work that they do. And it is hard, and it is difficult.

And we worry, I worry, about the morale of the men and the women for some of the same reasons that you have heard here today. I hope that the message that you convey back to them is that we need them to do the jobs that we have tasked them to do. We respect the work that they have in front of them. I was able to share my direct thanks.

I wanted to speak just very quickly to the issue that is really front and foremost in the minds of many people in Anchorage and around the State. Our State has been dubbed the most dangerous in the country, Anchorage as one of the more dangerous cities. You do not think about that when you think about Alaska, but the homicides on a per capita basis have put us in a category of notoriety that we do not seek, and we must address, and we must change.

We are seeing so much of this because of the drug violence that is coming with the trafficking that we are seeing. We are looking forward to what this high-intensity drug trafficking area program will bring to the area with some additional Federal resourcing. So any increased attention that we are able to receive when it comes to resourcing is pretty important, because we feel like we are at the end of the road there.

But I would ask your senior team to look at whether Alaska is being appropriately resourced to meet the Federal law enforcement needs in the State, and brief my office on the findings, specifically to coordinate with—we have a great U.S. attorney up there. We

have strong troopers. We need more of our troopers. Our police chiefs are maxed.

But it is really when all the partners come together that we are able to make some headway, and we capitalize on the resources that are made available.

So I would just ask your folks to take a look at that situation in Alaska, because, again, it has come on in unprecedented levels and at a time and a pace that is alarming to us.

Director WRAY. I would be happy to take a closer look at it. We have a great Special Agent in Charge up there, as you mentioned.

I do think, in general, these issues are going to be solved or mitigated through a combination of partnerships, as you alluded to, and intelligence partnerships meaning: How can we figure out how all the different players, the feds, FBI, the different Federal agencies, State and local agencies, can somehow get their 2-plus-2 to equal more than 4? In other words, how do we get synergies between them to maximize the impact? And the High Intensity Drug Trafficking Areas (HIDTA) designation that you described is part of that.

And then intelligence, meaning let's figure out what is really driving the problem and focus the resources on impact. I think all too often historically in law enforcement people focus just on stats of number of arrests, et cetera, without necessarily taking that next step to figure out if you are really addressing the core driver of the problem. Each city has its own unique idiosyncrasies.

We have gotten, I think, a lot better and, hopefully, can bring more to the table with our Intelligence Analysts to try to understand better what is it that is causing that spike that you are talking about in Anchorage.

Senator MURKOWSKI. Good. We look forward to working with you. Thank you for your leadership.

Thank you, Mr. Chairman.

Senator MORAN. Senator Murkowski, thank you very much.

Director, thank you very much for your testimony today, to this point.

I want to take a moment to reassure you and the people that you lead, but, more importantly, the American people, that we will do everything that we can as members of this subcommittee, as appropriators, and as United States Senators to see that the bureau is equipped to prevent and combat an ever-changing landscape both here and abroad of criminal activity that can be and has been very devastating to the American people.

We will take our responsibilities very seriously, and I look forward to developing a very close working relationship with you in that regard. And I appreciate the partnership that exists between the FBI and other Federal agencies, but particularly those agencies back home, my local and State law enforcement officials.

We have had significant success. I can name three off the top of my head just in the last few months in Kansas as a result of that partnership between the FBI and local law enforcement. So we are very grateful to you and to the men and women that you lead.

We are going to recess. My script says it is brief, but it will probably be longer than "brief."

ADDITIONAL COMMITTEE QUESTIONS

But with no further questions, this afternoon's open hearing is concluded. Senators may submit additional questions for the official record. We request the FBI's response within 30 days.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED TO HON. CHRISTOPHER A. WRAY

QUESTIONS SUBMITTED BY SENATOR JERRY MORAN

NATIONAL BIOFORENSIC ANALYSIS CENTER (NBFAC): DHS OWNED FACILITY USED BY FBI FOR BIOFORENSIC ANALYSIS—NEW COST SHARING ARRANGEMENT

Question 1. I understand that the FBI uses the National Bioforensic Analysis Center (NBFAC) for research and investigatory purposes. While the FBI is the main user of this facility, the lab itself is actually owned by the Department of Homeland Security. In order to avoid closure and maintain facility operations, the Bureau is considering sharing 40 percent of the NBFAC's expenses and operating costs with DHS.

1a. What is the nature of this agreement, including the work the FBI performs in this facility, and the importance of maintaining operations?

Answer. Since its inception in 2004, NBFAC was funded and operated by the Department of Homeland Security (DHS) and co-located with the Biological Threat Characterization Center (BTCC) in the National Biodefense Analysis and Countermeasures Center (NBACC) at Fort Detrick, Maryland. The NBFAC is a unique United States Government asset that permits the analysis of biological threat agents, including dangerous infectious agents and toxins, and examines traditional forensic evidence contaminated with biohazardous materials (e.g., fingerprints, trace evidence, documents, photographs, etc.). It is the only facility within the United States that can conduct these types of forensic analyses and examinations of biohazardous evidence. The NBFAC's capability ensures that the government is provided with high-quality, defensible, actionable results within hours or days instead of months or years, which was commonplace prior to the establishment of the NBFAC. Discontinuing operations would eliminate over 10 years of investment and progress in building a forensic analytical capability established to serve both law enforcement and the Intelligence Community in the examination of hazardous biological agents.

At the direction of the OMB, the FBI entered into a Memorandum of Agreement (MOA) to establish a cost-sharing agreement whereby the FBI provides 40 percent of the funds necessary for the operation of the NBACC. This MOA establishes the FBI as the responsible party for the operational activities of the NBFAC portion of the NBACC, while DHS retains its operation of the Biological Threat Characterization Center and the operation and maintenance of the NBACC building.

1b. Would it be more efficient for the FBI to own this facility itself and, if so, what would you expect the upfront and annual costs to be?

Answer. The FBI has not been asked to assume sole responsibility of the facility, and therefore, cannot provide a breakout of assumed costs.

1c. Finally, is this cost sharing arrangement included in the Bureau's budget request? Do you have sufficient resources to shoulder this agreement? Will the cost of NBFAC impact other aspects of FBI operations?

Answer. The fiscal year 2019 request was formulated before the Bipartisan Budget Act of 2018 was passed. As a result, the fiscal year 2019 request does not include any program increases for NBFAC. The FBI will attempt to minimize significant impacts to operations and will also work with other members of the biodefense community to develop a more expansive customer base and thus, offset overall costs.

COUNTERTERRORISM: FBI'S GROWING MISSION—RESPONSE V. POSITION REDUCTIONS

Question 2. Threats facing our Nation, both foreign and domestic, are evolving rapidly.

2a. What are the type of threats we are facing and how do they affect the growing mission of the FBI?

Answer. Preventing terrorist attacks remains the FBI's top priority. The terrorism threat to 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 and homegrown violent extremists as the main terrorism threats to the United States. Additionally, domestic violent extremist movements collectively pose a steady threat of violence and economic harm to the United States. As the threat to harm the United States and United States interests evolves, the FBI must adapt and confront these challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. The FBI uses all necessary lawful investigative techniques and methods to combat these terrorist threats to the United States.

2b. I am concerned by the Bureau's proposal to cut 500 positions in the fiscal year 2019 request, especially given that they are from the Intelligence; Counterterrorism and Counterintelligence; Criminal Enterprise and Federal Crimes; and Criminal Justice Services Divisions. The FBI must be good stewards of taxpayer dollars while having adequate resources to support its growing mission and responsibilities. Can you explain the proposed cuts included in the fiscal year 2019 request, addressing both the necessity and rationale?

Answer. As previously referenced, the fiscal year 2019 request was formulated before the Bipartisan Budget Act of 2018 was passed. As a result, the fiscal year 2019 request reflects a decrease of \$158 million. However, the FBI received significant increases in the fiscal year 2018 Appropriations to combat counterterrorism and counterintelligence, opioids, human trafficking, cyber intrusions, child exploitation, and surveillance, which must be sustained.

FIX NICS

Question 3.

3a. The Fix NICS Act was included in the 2018 Omnibus. What are the actions the FBI is taking to implement the Fix NICS Act?

Answer. The FBI has implemented the requirement to process appeals within 60 days of receiving the appeal. The FBI has provided guidance to the Point-of-Contact (POC) States regarding the adherence to the requirement under the Brady Handgun Violence Prevention Act of 1993 for processing appeals within the mandated timeframe.

Additionally, the FBI customized individual teleconferences with the States to raise awareness for reporting arrests to State repositories, relay the importance of submitting mental health records, provide support to the States in this endeavor, and to gain vital information from the States regarding their arrest and disposition reporting practices. Invitations were sent to the State CJIS Systems Officers (CSO), State Compact Officer (SCO), State Identification Bureau (SIB) Head, and NICS POC in each State to participate in their individual teleconference. Ten teleconferences a week were completed from April 9, 2018, through June 1, 2018. Only four United States Territories have not responded to their invitation, and the NICS Section is awaiting their response to schedule their teleconference. Additionally, the FBI is performing research to identify dispositions missing from criminal history records. Discussions are ongoing with the U.S. Courts and U.S. Attorney's Offices to develop a process for the electronic submission of dispositions.

The FBI also continues to coordinate with Federal agencies; since November 2017, eight new Federal agencies began submitting information to into NICS indices.

3b. The Fix NICS Act was included in the 2018 Omnibus, which passed after the FBI submitted its fiscal year 2019 budget request. Do you anticipate that the implementation of this Act will create new resource needs? If so, what are they?

Answer. The FBI has and continues to identify solutions to automate and streamline appeal-related processes. The NICS Section is cross-training staff and taking advantage of other personnel resources to support the NICS mission. The Fix NICS

Act includes a provision for the correction of erroneous system information within a 60-day timeframe from the date of receipt of information from an appellant for correction of erroneous information on a denied transaction.

Prior to the passage of the Fix NICS Act, there was no timeframe to complete an appeal after receiving information to correct an erroneous record on a denied transaction; therefore, implementation of the Fix NICS Act requirement to adjudicate appeals within 60 days of receipt could create resource challenges. The FBI has realigned resources to ensure it is processing appeals within the 60 day mandate.

In addition, the FBI will be conducting analysis to determine if every Federal agency has achieved benchmarks established in their implementation plans. This would require additional personnel and/or resources than what is currently dedicated. FBI resources would also need to be made available to Federal Departments or agencies that need technical assistance with compliance.

Further, the FBI will be required to provide training and technical assistance to all States.

3c. Finally, I understand that complete case records are often not included in the NICS system. Is there a way, either through implementing Fix NICS or otherwise to further incentivize State and local partners to update records in the NICS system, and include the final disposition of cases, following the initial report of an arrest?

Answer. The FBI relies upon the collaboration and cooperation of agencies nationwide to submit information on prohibited individuals. With the passage of the NICS Improvement Amendments Act of 2007 (NIAA), incentives were put in place to encourage local, State, and Tribal agencies to make eligible records available for NICS purposes through NICS Act Record Improvement (NARIP) grants. Likewise, the NIAA required Federal agencies to make relevant records available to the NICS. The National Criminal History Improvement Program (NCHIP) grant incentive also provides support to States for efforts to update records. The passage of the Fix NICS Act in March will further enhance these efforts. It requires States to provide an implementation plan by March 2019 with benchmarks for improvements as a needs assessment. This will further enhance the Department's efforts to identify obstacles in making complete records available to the NICS and what others steps can be taken to support State partners.

3d. What other actions is the Bureau taking to resolve this problem?

Answer. The list below describes steps the FBI is taking and has taken to encourage States to make available potentially prohibiting information for NICS determinations:

- Provide electronic interfaces for the ease and automation of record sharing;
- Provide detailed information, education, and liaison support to help agencies detect which records their agencies possess that would be of specific interest to the NICS;
- Provide regular and detailed reporting of records housed within the various databases of the FBI that each agency has submitted. These reports provide agencies a self-auditing tool that support the detection of missing records and/or incomplete data;
- The FBI staff are asked to speak at and support meetings and conferences nationwide. Subject matter experts support the efforts of State partners in making relevant records available at the national level;
- The FBI provides annual criminal history dashboards to agency contacts. Each dashboard provides information about the number of arrests on file in the FBI's Next Generation Identification (NGI) System, as well as the number of arrests with and without final disposition data;
- The FBI requests that agencies perform self-audits to identify gaps in providing arrests and subsequent disposition information to the NGI;
- The FBI provides reports to requesting agencies containing arrests with missing dispositions that are older than a year. This supports a continuous self-auditing tool;
- The FBI has dedicated staff performing research to assist in the location of missing dispositions, which the FBI then uses to update criminal history records in the NGI;
- The FBI has dedicated liaison teams who specialize with the applicable databases searched by the NICS. They provide regular and ongoing support to record-owning agencies and contributors with the identification, submission, and maintenance of data and records;

The FBI created a Disposition Task Force in 2009 and continues through today to collectively pursue methods to enhance disposition reporting.

CYBER SECURITY—THREATS AND CURRENT ASSESSMENT

Question 4. In the Director of National Intelligence's (DNI) Worldwide Threat Assessment, Cyber Security is again listed as the Top National Intelligence Priority. The FBI is the lead Federal agency for investigating cyber-attacks by criminals, adversaries, and terrorists.

4a. What are the threats we are currently facing and the actions the Bureau is taking to combat them, including the Bureau's "Going Dark" efforts?

Answer. The country faces cyber threats from sophisticated cybercriminals, cyberterrorists, and state-sponsored actors. The FBI has seen a rise in "blended threats," which are hybrid threats of nation states working in tandem with criminal actors to target the United States, its businesses, and its people. The Yahoo! Investigation is a recent example of this blended threat. FSB officers had protected, directed, and paid criminal hackers to collect information through computer intrusions in the United States and elsewhere. Similarly, in the Mabna Investigation, nine Iranians were charged with conducting a massive cyber theft campaign against educational, private, and government institutions on behalf of the Islamic Revolutionary Guard Corps. These individuals were each leaders, contractors, associates, hackers-for-hire, or affiliates of the Mabna Institute, an Iran-based company.

The United States also faces the significant issue of threats to Critical Infrastructure. Cyber attacks against the energy sector can cause significant disruptions or damage to the industrial control systems/supervisory control and data acquisition (ICS/SCADA) systems. Advanced persistent threat (APT) actors can harvest credentials and establish persistence on victim energy sector networks with the intent to develop cyber-attack capabilities or cause energy service disruptions during conflict. Similar APTs exist targeting the telecommunications and financial services sectors.

One of the most significant challenges to the FBI's ability to access investigative data is the "Going Dark" problem. "Going Dark" describes circumstances where the government is unable to obtain critical information in an intelligible and usable form (or at all), despite having a court order authorizing the government's access to that information. The problem impacts a range of issues, including: data retention; anonymization; provider compliance (or absence thereof); real-time communications; foreign-stored data; data localization laws; tool development and perishability; and other similar issues. Impacting the FBI's investigative and intelligence programs. Electronic communication service providers are increasingly implementing encryption in a manner to thwart court ordered government access to the content of communications. Counterterrorism and counterintelligence subjects are extensively using encryption technologies to conceal their communications and nefarious activities. Drug trafficking organizations are using anonymization and encryption technologies to obfuscate and expand their criminal interests; further contributing to the opioid crisis. Gangs, organized crime, human trafficking rings, and child exploitation offenders use anonymization and encryption technologies to inhibit investigative efforts to identify and prevent these horrific crimes. In an effort to address these Going Dark challenges, the FBI created a new Section (Cyber Operations Section) which will be responsible for computer network exploitation capabilities and enabling innovation.

The FBI is open to all constructive solutions that seriously address the public safety issues. We need a thoughtful and sensible approach, one that may vary across business models and technologies. We have a team devoted to explaining this challenge and are currently working with stakeholders to find a way forward.

4b. The fiscal year 2019 request does not include any program enhancements for cyber and other mission activities. Is the Bureau adequately equipped to combat the growing number of cyber-attacks?

Answer. The FBI is committed to its mission of protecting the American people and will align resources to the highest priority threats, including cyber attacks, dangerous gangs and the opioid crisis.

Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. The FBI faces sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek state secrets, trade secrets, technology, and the ideas of the American people—things of incredible value and of great importance to the conduct of government business and national security. They also seek to strike critical infrastructure and to harm the United States economy.

The FBI is 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. The FBI also continues to actively coordinate with private and public partners to pierce the veil of anonymity surrounding cyber based crimes.

The FBI is engaged in a myriad of efforts to combat these cyber threats, from improving threat identification and information sharing inside and outside of government to developing and retaining new talent, to examining the way the FBI operates to disrupt and defeat these threats. The FBI takes 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.

FBI INVESTIGATION OF USA GYMNASTICS

Question 5. I chair the Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, which has oversight jurisdiction over Olympic and amateur sports through the Ted Stevens Olympic and Amateur Sports Act. Because hundreds of current and former athletes have come forward with accusations of abuse by individuals associated with their sports, my Commerce Subcommittee launched an investigation into the United States Olympic Committee (USOC), USA Gymnastics (USAG), and Michigan State's responses to the claims of sexual abuse of young athletes, which include the abuse inflicted by former sports doctor Larry Nassar. Documents obtained by my Commerce Subcommittee and outside reports indicate that the FBI was made aware of accusations against Nassar as early as July, 2015.

5a. What is the FBI's role in investigating these crimes, and did the Bureau share the reported accusations it received or its own investigatory findings with State or local law enforcement?

5b. Did the FBI share the details of the accusations or its investigatory findings with Michigan State prior to September, 2016? If not, why?

5c. It has been reported that the FBI asked USA Gymnastics to keep these accusations of abuse private, is that true? If so, why?

5d. Finally, what role do you see the FBI playing to protect future athletes from abuse that may cross State jurisdictions and what resources does the FBI need to fill this role?

Answer to all portions of Question 5. Until an on-going review being conducted by FBI Inspection Division is completed, the FBI will not provide comment.

QUESTION SUBMITTED BY SENATOR SUSAN M. COLLINS

Question 1.

1a. As Chairman of the Senate Aging Committee, I have held numerous hearings focused on scams and fraudulent schemes that target our Nation's seniors. I'm pleased to see that the FBI is directing people to the Aging Committee's website for additional resources, including our Fraud Hotline. Seniors lose an estimated \$3 billion annually to financial exploitation, and the perpetrators of these scams are sophisticated and ruthless. The FBI initiated more than 200 cases involving financial crimes against seniors in the last year, and it played an important role in the elder fraud sweep recently announced by the Attorney General that involved over 250 defendants and losses of more than half a billion dollars. The Aging Committee's own data show that recent arrests have had a real impact on deterring scammers. How is the FBI directing resources toward combatting these crimes, including by working towards gaining more cooperation from countries where these criminals are operating?

Answer. Combatting elder fraud is a Department of Justice priority. As a part of the Department of Justice's elder fraud initiative, the largest coordinated sweep of elder fraud cases in history took place in February 2018. The cases involve more than 250 defendants from around the globe who victimized more than a million Americans, most of whom were elderly. The cases include criminal, civil, and forfeiture actions across more than 50 Federal districts. Of the defendants, 200 were charged criminally. In each case, offenders engaged in financial schemes that tar-

geted or largely affected seniors. In total, the charged elder fraud schemes caused losses of more than half a billion dollars.

Exceptional assistance from foreign law enforcement partners has amplified the effectiveness of the Department's initiative. The sweep in February 2018 benefited greatly from the work of the International Mass-Marketing Fraud Working Group (IMMFWG), a network of civil and criminal law enforcement agencies from Australia, Belgium, Canada, Europol, the Netherlands, Nigeria, Norway, Spain, the United Kingdom, and the United States. The IMMFWG is co-chaired by the United States Department of Justice and FTC, and law enforcement in the United Kingdom, and serves as a model for international cooperation against specific threats that endanger the financial well-being of each member country's residents.

As the lead Federal criminal agency for the investigation of financial crimes, the FBI will continue to prioritize our efforts to protect all citizens, including our seniors, not only through law enforcement efforts, which are a large deterrent, but also through partnerships with other criminal and civil agencies. One of our main goals is to ensure we inform and educate the public on these criminal actors who seek to take advantage and swindle innocent victims of their hard earned savings.

The FBI also works closely with our international partners to support investigations with an international nexus through our 63 Legal Attaché offices around the world and through specific initiatives such as the recent Operation Wire Wire which addressed financial crimes in partnership with Nigeria.

In a focused effort to combat elder fraud, the FBI will continue to work closely with the Department of Justice to ensure agents are trained to identify and investigate elder fraud schemes. The FBI has over 700 agents dedicated to addressing a variety of financial crimes, including many which affect the elderly. Currently there are over 6,000 active financial crime investigations.

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

ONGOING RUSSIAN ELECTORAL INTERFERENCE IN 2018

Question 1. The FBI was among the 17 intelligence organizations concluding that Russian President Vladimir Putin ordered a multi-pronged influence campaign aimed at sowing discord among the American electorate and helping to elect Donald Trump. Now we are just months away from the 2018 midterm elections.

1a. What is the FBI's assessment about the threat of Russia again trying to interfere in our elections? What is the FBI doing to combat this interference, and what more needs to be done?

Answer. To ensure the FBI is positioned to protect our democratic processes in advance of the upcoming 2018 and future elections, we have undertaken numerous efforts in collaboration with partners in the United States and abroad. Notably, the FBI established the Foreign Influence Task Force in the fall of 2017 to identify and combat foreign influence operations targeting the United States.

The FBI will continue to work with our United States Government and international partners to identify and disrupt, as appropriate and lawfully authorized, foreign activities aimed at interfering with our democratic process and will raise public awareness about the objectives and tactics of foreign adversaries seeking to influence the information environment.

The FBI does not have any information suggesting Russia will cease its attempts to interfere with United States elections or to otherwise attempt to undermine public confidence in United States democratic institutions.

ZTE

Question 2. At the May 22, 2018, hearing, I asked you about the threat posed to our national security by the Chinese telecommunications company ZTE. You testified that you are "deeply concerned" about the threat posed by companies beholden to adversarial foreign powers, such as ZTE.

2a. Given President Trump's order to the Commerce Department to get ZTE "back into [sic] business fast,"¹ will you commit to conveying your concerns about ZTE to the National Security Advisor or other White House officials as appropriate?

Answer. As we've previously stated, Chinese firms such as ZTE and Huawei seek to gain access to critical United States telecommunications infrastructure through

¹ <https://twitter.com/realdonaldtrump/status/995680316458262533?lang=en>.

the sale of equipment, service agreements, acquisitions, and joint ventures. While these firms may be motivated in part by commercial interests, some of these transactions could give the government of China the capacity to exert pressure or control over United States telecommunications infrastructure, maliciously modify or steal information from government and corporate entities, and conduct undetected espionage against the United States Government and private sector interests.

The FBI remains committed to informing the private sector and United States Government officials about these potential risks to national security and working with these stakeholders to assess the risk created by particular commercial relationships and ensure that these risks are factored into related decisions. We have also informed appropriate government agencies of specific risks.

CITIZENSHIP ALONE AND THREAT OF TERRORISM

Question 3. I have asked several Trump administration officials whether they agree with a 2017 Homeland Security Office of Intelligence and Analysis report that found that citizenship alone is *not* a reliable indicator of terrorist threat. These officials, including your predecessor Director Comey and then-Secretary of Homeland Security John Kelly, told me they agree with the report's conclusion.

3a. Do you agree that citizenship alone is not a reliable indicator of terrorist threat?

Answer. Yes, citizenship alone is not a reliable indicator of terrorist threat.

TORTURE

Question 4. I asked you at your confirmation hearing if waterboarding was torture and you said that it was. This question is more timely than ever because our President has talked about bringing back waterboarding and “a hell of a lot worse.”

4a. In your view, does a human being have a moral right not to be tortured?

Answer. As I have stated during previous congressional testimony, torture is illegal under Federal law. The FBI will not engage in torture.

BUDGET REQUEST

Question 5. The President's budget request reduces overall FBI funding by 5 percent, requests no funding for the new FBI headquarters, and requests a rescission of another \$148 million in salaries and expenses.

5a. How will these proposed cuts impact the FBI's ability to meet its law enforcement, investigatory, and national security mission?

Answer. The fiscal year 2019 request was formulated before the Bipartisan Budget Act of 2018 was passed. As a result, the fiscal year 2019 request reflects a decrease of \$158 million from the 2018 enacted level for Salaries and Expenses. This Committee provided significant increases in the fiscal year 2018 Appropriation, including resources to combat terrorism, counterintelligence, opioids, human trafficking, cyber intrusions, child exploitation, and surveillance, which must be sustained.

STINGRAYS/CELL SITE SIMULATORS

Question 6. In 2015, the Department of Justice issued guidance on the use of cell site simulators, also known as “Stingrays,” requiring a warrant to use this invasive technology.² Federal law requires simulators to be operated with minimum interference to cellular service.³ But there have been reports that Stingrays may interrupt cellular service—including disrupting 911 calls. It is important that when the FBI seeks a court order for use of a Stingray, it fully informs the court about any interference this technology may cause.

6a. What data or information does the FBI rely upon to ensure that its use of Stingrays generates “a minimum of interference”—as required by law?

Answer. The FBI has developed law enforcement sensitive operational protocols and device configurations designed to permit the operation of cell site simulators (CSS) with a minimum of interference in accordance with our legal obligations under Title 18, United States Code, section 3124. In developing the protocols and

² <https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators>.

³ 18 U.S.C. § 3124.

settings, the FBI has leveraged the expertise of engineers who have extensive experience in cellular networks. Decades of successful CSS use by the FBI and other agencies have validated the FBI's position with respect to minimizing the potential for interference.

ENCRYPTION

Question 7. The FBI is reportedly renewing a push for legal authority to force U.S. technology companies to build decryption tools into smartphones and other devices.⁴ I am concerned this sort of “exceptional access” system would introduce inherent vulnerabilities and weaken security for everyone, but I am also concerned about what effects this will have on U.S. technology and those that use it.

7a. If we require U.S. device manufacturers to build encryption “backdoors” into their products, won’t that simply harm our world-leading technology companies by encouraging innovation elsewhere, like Germany or Finland?

Answer. The FBI is not seeking to force companies to include specific technology mandates, sometimes wrongly referred to as “backdoors,” into products and services, and we recognize and support the use of encryption to make Americans safer. However, the FBI does not view the encryption debate as a “zero sum” issue, where there is either total encryption that prevents anyone from accessing data for any reason or no encryption.

7b. If we require U.S. technology companies to build “backdoors” into their products, then what do you expect Apple to do when the Chinese government demands that Apple help it unlock the iPhone of a peaceful political or religious dissident in China?

Answer. As stated above, the United States does not seek “backdoors.” While we cannot presume to know the details of the specific proprietary agreements between Apple and China in which China approved the sale of Apple products, it is important to note that the Chinese government’s domestic law only permits the sale or use of products in China that use government-approved encryption technology. Any companies or individuals selling encryption products in China must first obtain the approval of the government, and to obtain that approval, legal requirements require companies to provide source code to computing and network equipment. Finally, China’s anti-terrorism laws require all data related to Chinese users to be maintained on servers in China and companies to provide encryption keys to public security authorities, so China would not need Apple’s assistance in unlocking their products.

BORDER SEARCH OF ELECTRONIC DEVICES

Question 8. Senator Daines and I recently introduced legislation that would require the Department of Homeland Security to have at least reasonable suspicion when they search the electronic devices of Americans at an international border crossing. Current DHS policy allows DHS officers to conduct such searches for no reason at all, under the so-called “border search exception” to the Fourth Amendment’s warrant requirement.

8a. If the FBI were to conduct a search of an American’s electronic device at the border, what level of probable cause or reasonable suspicion would Bureau policy first require?

Answer. The FBI is required to follow the controlling legal authority in each Federal jurisdiction where the authorized investigative activity occurs.

QUESTIONS SUBMITTED BY SENATOR DIANNE FEINSTEIN

MCCABE MEMOS

Question 1. The Washington Post has reported that former FBI Deputy Director Andrew McCabe kept notes and wrote memos detailing his interactions with the President.

1a. Is this accurate—did Mr. McCabe take contemporaneous notes or write memos about his interactions with the President?

1b. Will the FBI also provide Mr. McCabe’s notes and memos?

⁴ <https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html>.

Answer. The FBI cannot confirm or deny the accuracy of the Washington Post's reporting because doing so may implicate an ongoing investigation.

TORTURE REPORT AND THE FBI

Question 2. In 2014, the Senate Intelligence Committee's Study of the CIA Detention and Interrogation Program was completed and a copy of the full 6,700-page classified report was sent to parts of the executive branch, including the FBI.

The Study is intended to be used broadly by those with appropriate clearances to ensure that the abuses documented in the Study would never be repeated.

2a. Have you personally read the Study? If not, will you commit to reading it?

2b. Have other top-ranking FBI officials read the Study? If not, will you ensure that the full, final Study is reviewed by top FBI officials?

Answer. I am familiar with the critical portions of the study, including the findings and conclusions. As I have stated during previous congressional testimony, torture is illegal under Federal law. The FBI will not engage in torture.

DOMESTIC VIOLENCE CRIMES AND GUNS

Question 3. Individuals convicted of domestic violence abuse or who are subject to a protection order are supposed to be prohibited from possessing firearms or ammunition under Federal law.

However, I understand that many domestic violence abusers are, nevertheless, able to buy guns. In 2013 and 2014, 30 percent of denials for misdemeanor crimes of domestic violence were issued after the prohibited abuser took possession of the firearm, because the background check was not completed in time.

It is important for the FBI to partner with local law enforcement and domestic violence programs to reduce the number of firearms in the hands of domestic violence offenders.

3a. What is the FBI doing to reduce firearm possession by domestic abusers?

Answer. The National Instant Criminal Background Check System (NICS) makes every effort to make Misdemeanor Crime of Domestic Violence (MCDV) determinations within three business days, before a firearm transfer is allowed under Federal law. Because the MCDV force element and relationship to victim may not be readily apparent in an automated record found during the NICS background check process, the NICS Legal Instruments Examiner (NICS Examiner) must reach out to external agencies to obtain this needed information. As a result, transactions involving a potential MCDV conviction are frequently delayed for further research. In order to be prohibiting, the NICS Examiner must determine the existence of a requisite qualifying relationship, as well as establish if the individual was convicted of an offense or subsection of an offense, which has an element of use or attempted use of physical force, or threatened use of a deadly weapon.

The FBI continues to pursue initiatives that allow for accurate and complete information to be available to the NICS. With the passage of the NICS Improvement Amendments Act of 2007, Congress instituted incentives and requirements to assist local, State, Tribal, and Federal agencies in making eligible records available for NICS purposes. The FBI has long-standing relationships with record-owning agencies, and has collaborated with and advocated for record sharing. The FBI has numerous proactive measures in place to support agencies in the identification of lacking or missing information in the applicable databases searched by the NICS. The bulleted list below highlights a few specific measures the FBI has in place to address missing or incomplete records in the applicable databases searched by the NICS. Particular attention has been given to the criteria needed to identify disqualifying MCDVs, not only by the FBI, but by Federal agencies awarding grant money in support of record improvement.

- Educational outreach to increase database records and final dispositions, as well as the identification of other needed pieces of information to support the immediate identification of prohibiting information, such as relationship to victim, statute, and subsection of the conviction;
- The FBI provides annual criminal history dashboards to agency contacts. Each dashboard provides information about the number of arrests on file in the FBI's Next Generation Identification (NGI) System, as well as the number of arrests with and without final disposition data;
- The FBI requests that agencies perform self-audits to identify gaps in providing arrests and subsequent disposition information to the NGI System;

- The FBI provides reports to requesting agencies containing arrests with missing dispositions that are older than a year. This supports a continuous self-auditing tool;
- The FBI has dedicated staff performing research to assist in the location of missing dispositions, which the FBI then uses to update criminal history records in the NGI;
- The FBI has dedicated liaison teams who specialize with the applicable databases searched by the NICS. They provide regular and ongoing support to record-owning agencies and contributors with the identification, submission, and maintenance of data and records;
- If an MCDV is established by the FBI and all the needed criteria cannot be added to the appropriate criminal history record, a record is added to the NICS Indices to support future transactions. State users of the NICS have been likewise encouraged to do the same.

In addition, there are various tools available to contributors to indicate a person's ineligibility. For example, in the NCIC, a contributor could set a Brady Indicator within the protection order record, or a condition set by the judge that would immediately indicate a person's disqualification. Within the criminal history record, a contributor could be sure to post the specific section/subsection of the subject's conviction, post the relationship to victim information on the face of the record, or set the firearm's disqualification flag. All of these practices serve the immediate nature with which the NICS Section is intended to serve. The FBI has and continues to educate and promote these tools to all criminal justice partners.

HANDGUNS THAT FIRE RIFLE ROUNDS

Question 4. Over the past two decades, the gun industry has developed handguns that can fire rifle rounds, which can penetrate the standard body armor worn by law enforcement officers. This is extraordinarily concerning to our law enforcement officers and to everyday citizens.

4a. Do you believe such handguns that can fire rifle rounds represent a threat to law enforcement?

Answer. Any handgun used in a crime of violence against law enforcement officers is a threat. These specific handguns—which fire traditional rifle caliber cartridges—are especially dangerous due to the high likelihood of the projectile penetrating traditional soft body armor. However, the FBI does not have the pertinent data to quantify the specific increased threat.

4b. What is the FBI's plan to address this new type of weapon?

Answer. The concern is not the weapon but rather cartridge and subsequent projectile which a weapon fires. The FBI has long been focused on identifying cartridges which create the highest threats to FBI personnel. In identifying these threat cartridges, the FBI has invested heavily in “rifle rated plates” for issuance to our personnel. These plates greatly reduce the risk of armor penetration by rifle caliber rounds to the most vital areas.

The FBI shares information on this threat with State and local authorities through established partnerships between the Training Division's Ballistic Research Facility (BRF) and the Academy's executive leadership programs.

HATE CRIMES

Question 5. While the FBI typically reports 7,000 to 10,000 hate crimes, the Bureau of Justice Statistics estimates that the true number may approach 300,000, approximately 30 times more.

Unfortunately, the number of State and local law enforcement agencies reporting their hate crimes statistics to the FBI seems to be decreasing, with 500 fewer agencies reporting their data to the FBI between 2014 and 2015.

5a. What do you intend to do to make it easier for local agencies to report this crucial data to the FBI?

Answer. The FBI is in the process of transitioning all law enforcement agencies (LEAs) to the National Incident-Based Reporting System (NIBRS) by January 1, 2021. Reporting via NIBRS will improve the quality, reliability, and accuracy of the data received from participating LEAs. NIBRS will also ease the ability for LEAs to report hate crime data as it is collected within the NIBRS record layout versus a separate record layout which is required for Summary Reporting System agencies.

The FBI is actively participating in the Department of Justice's (DOJ) Hate Crime Enforcement and Prevention Initiative. This group is focusing on developing strate-

gies for improving the hate crime data collection. One strategy developed is a plan to offer joint law enforcement officer (LEO) hate crime training throughout the country with the assistance of the FBI Civil Rights Unit (CRU). The FBI will assist the LEO participants in understanding the Federal hate crime laws and identifying bias-motivated incidents. Ensuring the officers at a crime scene, and/or officers interviewing the victim(s) have a full understanding of the events which occurred within a bias-motivated incident is essential to identify these crimes.

There is also an additional focus on how LEAs report hate crime data to the FBI. To emphasize the importance and value of reporting hate crime data, the FBI is currently contacting State UCR Program managers, requesting that State-sponsored training conducted by the FBI is carried out within that managers' region. In addition, the FBI posts information about hate crimes on the publicly available web site at <<https://ucr.fbi.gov/hate-crime/>>

5b. What do you think would foster more accurate and complete reporting from local police to the FBI?

Answer. The FBI believes obtaining the commitment of local agency administrators to provide hate crime investigative training to their LEOs would foster more accurate and complete reporting. Many officers may not be aware of the signs to look for when investigating a bias-motivated crime. Often times, a hate crime incident requires additional investigation to ascertain if the offense was motivated by the offender's bias against the victim. Instituting a hate crime point of contact or unit within the LEAs could also improve the reporting of hate crime incidents.

WHITE NATIONALISM AND ONLINE CYBER-HATE

Question 6. During last year's Presidential election, the Anti-Defamation League identified 2.6 million tweets that had anti-Semitic language, with nearly 20,000 tweets directed at 50,000 U. S. journalists.

One Jewish reporter received threats over twitter, including a picture of her face superimposed on a corpse in a concentration camp. The photo included a message saying, "Don't mess with our boy Trump, or you will be first in line for the camp." This type of cyber-hate has targeted other minority communities as well, including Muslim and immigrant communities.

6a. What steps is the FBI taking to address the rise of these threatening messages and prevent them from leading to actual hate crimes?

Answer. Hate crimes are the highest priority of the FBI's Civil Rights program, not only because of the devastating impact they have on families and communities, but also because groups that preach hatred and intolerance can plant the seed of domestic terrorism here in our country. As part of its responsibility to uphold and protect the civil rights of the American people, the FBI takes a number of steps to combat hate crimes. The Bureau investigates hundreds of these cases every year and works to detect and deter further incidents through law enforcement training, public outreach, and partnerships with a myriad of community groups.

The FBI is the lead investigative agency for criminal violations of Federal civil rights statutes. The FBI works closely with State/local/Tribal authorities on investigations, even when Federal charges are not brought. FBI resources, forensic expertise, and experience in identification and proof of hate-based motivations often provide an invaluable complement to local law enforcement.

The FBI has forged partnerships nationally and locally with many civil rights organizations to establish rapport, share information, address concerns, and cooperate in solving problems. Additionally, the majority of the FBI's field offices participate in local Hate Crime Working Groups. These Working Groups combine community and law enforcement resources to develop strategies to address local hate crime problems.

The FBI conducts hundreds of operational seminars, workshops, and training sessions annually for local law enforcement, minority and religious organizations, and community groups to promote cooperation and reduce civil rights abuses. Each year, the FBI also provides hate crimes training for new agents, hundreds of current agents, and thousands of police officers worldwide.

6b. Is the FBI working with social media companies to take down these types of messages and posts?

Answer. The mission of the FBI's Civil Rights program is to enforce Federal civil rights statutes and to ensure the protected rights of all persons are not violated. This requires a delicate balance between the enforcement of hate crimes statutes and a rigorous obedience to the Constitution of the United States.

A hate crime is defined as a criminal offense against a person or property motivated by the individual's bias against race, religion, disability, ethnic/national origin, sexual orientation, gender, or gender identity. The FBI must pursue its legitimate investigative goals without infringing upon the protected exercise of free speech. In the absence of an allegation of a violation of Federal law, the FBI cannot pursue investigative activities. When a message or post sent via social media rises to the level of a true threat as defined by the Supreme Court of the United States, that is, when a message communicates a serious intent to commit an act of unlawful violence against an individual or group, based on the aforementioned protected classes, the FBI can initiate a hate crime investigation. In the course of that investigation, the FBI may request a social media company preserve the threatening post as evidence. A post containing a threatening message sufficient for the FBI to open a hate crime investigation would likely also violate the terms of service of any established social media company.

QUESTIONS SUBMITTED BY SENATOR JACK REED

FOREIGN MEDDLING IN AMERICAN ELECTIONS

Question 1. Since the Citizens United decision, our campaign finance system has been inundated with dark money, or funds donated to entities that may conceal the identities of donors, which are in turn spent to influence our elections. Now, it has been reported that the FBI is investigating allegations that malign Russian interests have used our broken campaign finance system to conceal allegedly illegal campaign finance activity with the aim of influencing American elections.

1a. What legal or institutional obstacles exist that could frustrate law enforcement officials' ability to identify all beneficial owners or other participants in a scheme to funnel foreign money into the American campaign finance system?

Answer. Companies founded under section 501(c)(4) of the Internal Revenue Code are not required to disclose their donors to the Internal Revenue Service and can accept unlimited contributions without disclosing the source of funds. 501(c)(4) and limited liability companies (LLC) can then be used to make political expenditures themselves or donate to Super PACs, potentially influencing elections while avoiding the required transparency of campaign finance laws, which increases the risk that they can be used illegally to funnel foreign money into U.S. Federal elections.

1b. In the course of investigating criminal foreign election meddling, would law enforcement benefit from greater transparency as to the identities of all persons behind transfers of otherwise dark money in the American campaign finance system?

Answer. Adding transparency laws to common non-profit schemes utilized by dark money brokers would allow law enforcement to more easily identify potential foreign influence schemes by forcing the identities of sources of funds to be disclosed.

QUESTIONS SUBMITTED BY SENATOR CHRIS VAN HOLLEN

Question 1. What specific actions has President Trump directed you to take to investigate and confront Russian interference in future U.S. elections, including to prevent Russian cyber-attacks on voting infrastructure and State-sponsored disinformation efforts through media?

1a. Has the President taken actions sufficient to deter Russian interference in future U.S. elections?

Answer. The FBI has undertaken numerous efforts in collaboration with our counterparts in the United States Government and international partners to protect our democratic processes.

The threat of foreign interference in our democratic process through the weaponization of the information space requires a whole-of-society response. The FBI's efforts are focused on identifying, and when possible and appropriate, exposing covert foreign sponsorship of disinformation, propaganda, and broader influence operations.

1b. Has the President committed additional resources to the FBI's efforts to investigate and prevent Russian interference in U.S. elections? If yes, please describe how the FBI is utilizing those resources to confront future interference in U.S. elections.

Answer. In fiscal year 2018, the FBI created a Foreign Influence Task Force to investigate efforts by foreign actors to influence threats to the electoral process. Intelligence gleaned from Task Force efforts are shared with Intelligence Community partners.

Question 2. The fiscal year 2018 omnibus funds the Criminal Justice Services at \$540 million. The Criminal Justice Services unit houses the Criminal Justice Information Services (CJIS) Division whose mission is to “equip law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the U.S. while preserving civil liberties.” CJIS operates the Next Generation Identification (NGI) which has processed approximately 76 million fingerprints each year in the past 2 years; the National Instant Criminal Background Check System (NICS) which allows Federal Firearm Licensees (FFLs) to conduct instant criminal background searches on firearm sales and the Uniform Crime Reporting (UCR) program which provides statistical compilations of crimes such as murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson; officers killed and assaulted in the line of duty; and hate crime statistics.

The FBI’s fiscal year 2019 budget proposes \$503.364 million dollars for CJIS which represents a \$36.636 million cut.

The FBI has stated in its fiscal year 2019 budget justification that it plans to reform the UCR to ensure a national standard for reporting crime.

2a. The FBI created a New UCR Project with the goal to “improve the accuracy and timeliness of the crime data collection and delivery process” and to have NIBRS become the national standard for crime reporting by January 1, 2021. How will the FBI accomplish this goal with these budget cuts?

Answer. In January 2018, the Federal Bureau of Investigation (FBI) surged subject matter experts with established skill sets to define a way forward to transition agencies reporting crime via the Summary Reporting System to the NIBRS. For agency planning purposes, 2018 is considered a pivotal year for the NIBRS transition. The FBI is executing critical engagement activities in the areas of (1) NIBRS transition data, (2) stakeholder engagement, and (3) marketing. The submission of crime data to the FBI is voluntary and agencies’ transitions to NIBRS are affected by many variables outside of the FBI’s direct control. The FBI is encouraging agencies to take these steps, which should result in the progression toward a national NIBRS transition. Specific strategies currently being executed by the FBI include:

- Monitoring the overall progress of the transition on an agency level.
- Engagement with State and Federal Uniform Crime Reporting (UCR) Program administrators.
- Engagement with law enforcement associations and other representative groups, to include, but not limited to:
 - Criminal Justice Information Services (CJIS) Advisory Policy Board (APB),
 - International Association of Chiefs of Police,
 - Major Cities Chiefs Association,
 - National Sheriffs’ Association, and
 - Major County Sheriffs of America.
- Leveraging FBI Field Offices to promote the importance of the transition to NIBRS with partner agencies in their areas of responsibility.
- Partnering with the Department of Justice, Bureau of Justice Statistics to increase NIBRS participation by offering funding assistance through the National Crime Statistics Exchange initiative.
- Development of preeminent UCR and NIBRS Web sites with comprehensive NIBRS transition resources.

In the fall of 2017, the FBI assembled a task force, comprised of FBI personnel and local, State, Tribal, and academia representatives, to address crime-reporting timeliness and provide recommendations on how to obtain and release data in a timelier manner. The recommended changes allow for the most frequent updates of crime data to be released.

On June 30, 2017, the FBI deployed the Crime Data Explorer (CDE), an additional part of the FBI’s effort to modernize the publication of national crime data. CDE allows the public to view and interact with FBI data, providing users with the ability to query, view, and download crime-reporting data submitted to the FBI.

In June 2018, the FBI deployed the Uniform Crime Reporting-Technical Refresh (UCR-TR), allowing for enhancements in the processing of crime data. UCR-TR is a centralized, searchable data repository of the FBI. One major enhancement the UCR-TR provides is the automation of data processing, which until the system’s de-

ployment was manually conducted by the FBI. The following are some of the functions UCR–TR provides:

- Supports new and legacy data submitted through NIBRS, Summary Reporting, Law Enforcement Officers Killed and Assaulted (LEOKA), and Hate Crime, automating manual data quality processes.
- Establishes interoperability by providing the capability to receive data submission in a modern data specification (i.e. extensible markup language [XML]).
- Provides an internal web-based interface for FBI users to access data to improve service to UCR data contributors.
- Supports an external web-based portal, the CDE, to provide data dissemination to law enforcement agencies and the public to allow for electronic publishing on a more frequent schedule.

The deployment of the CDE combined with the NIBRS transition, UCR–TR, and the cessation of the data embargo policy will improve the accuracy and timeliness of the collection and release of crime data.

2b. In 2015, then Director Comey said that it was ‘unacceptable’ that the Guardian newspaper had better data on police violence than the FBI did. Do you also agree that this is unacceptable?

Answer. High profile events involving the law enforcement community and public highlighted the need for better crime data. In order to address this need, the FBI established the National Use-of-Force (UoF) Data Collection at the behest of local, State, Tribal, and Federal partners and major law enforcement agencies. The National UoF Data Collection is a voluntary collection in which local, State, Tribal, and Federal agencies provide the FBI with information on incidents of use-of-force. The goal of the data collection is not to offer insight into single use-of-force incidents, but to provide an aggregate view of the incidents reported and the circumstances, subjects, and officers involved.

2c. Do I have your commitment that the new NIBRS metric will include data on the use of excessive force by police officers?

Answer. The FBI is committed to implementing the National UoF Data Collection. While this collection is a separate collection from the NIBRS, both collections reside within the FBI’s UCR Program. The National UoF Data Collection will include any use-of-force which results in the death or serious bodily injury of a person, as well as when a law enforcement officer discharges a firearm at or in the direction of a person. The definition of serious bodily injury will be based, in part, upon Title 18, United States Code, Section 2246 (4). The term “serious bodily injury” means “bodily injury that involves a substantial risk of death, unconsciousness, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental faculty.”

The FBI is working with the Office of Management and Budget on the release of this national collection.

Question 3. An analysis by FiveThirtyEight, revealed that “the 2016 Crime in the United States report—the first released under President Trump’s administration—contains close to 70 percent fewer data tables than the 2015 version did.” Four of my colleagues and I sent a letter to you and AG Sessions asking you to restore this data and I am pleased that the missing data sets have been restored. However, I remain concerned. The FBI’s response indicates that you performed an analysis of web traffic data and eliminated the data sets that were not frequently trafficked and thus reduced publicly available data from 81 to 29 tables. Policymakers, criminologists, researchers and the public rely on this objective data to analyze crime trends.

3a. What prompted the FBI to conduct this web traffic review? Is this the first time such a review has been conducted regarding crime data sets?

Answer. In an effort to move to a digital presentation of data, FBI staff performed web traffic analysis on tables viewed in previous Crime in the United States (CIUS) reports. This was the first time the FBI had conducted such an analysis. Many of the eliminated tables were different views of the same data set. Based on user feedback, the FBI published all 74 tables as downloadable Excel files on FBI.gov. These files were made available to the public on April 19, 2018.

3b. Do I have your commitment that you will retain all data sets going forward to ensure transparency?

Answer. The Crime Data Explorer (CDE) is part of the FBI’s broader effort to modernize the reporting of national crime data. CDE is a web-based solution ena-

bling the public to view and interact with the FBI data in an intuitive and user-friendly way. The FBI plans to leverage the CDE to transition from a table driven publication to a more accessible view of the data. CDE users can view trends, download bulk datasets, and access an open application-programming interface, which allows users to create custom views and conduct their own analysis of the data reported to the FBI.

A marketing strategy will be implemented to ensure the public is aware of how to access the data.

SUBCOMMITTEE RECESS

Senator MORAN. The subcommittee now stands in recess. We will reconvene in a closed and classified session to hear Director Wray in SVC-217.

I intend to call that meeting to order shortly after the beginning of the second vote now occurring in the United States Senate. Thank you.

[Whereupon, at 3:36 p.m., Wednesday, May 16, the subcommittee was recessed, to reconvene subject to the call of the Chair.]