Department of Justice

STATEMENT OF

JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

FOR A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

MAY 3, 2017

Statement of
James B. Comey
Director
Federal Bureau of Investigation

Before the
Committee on the Judiciary
United States Senate

For a Hearing Entitled
"Oversight of the Federal Bureau of Investigation"

May 3, 2017

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

Today's FBI is a 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.

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

National Security

Counterterrorism

The FBI's top priority is protecting the American people from terrorist attack. From a threat perspective, we are concerned with three areas in particular: (1) those who are inspired by the terrorists' 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.

In this endeavor, our main focus is the so-called Islamic State — the group we refer to as ISIS. ISIS has proven relentless in its campaign of violence and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. Though many foreign terrorist organizations use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to extremist messages, no group has been as successful at drawing people into its perverse ideology as ISIS. ISIS's extensive reach through the Internet and social media is most concerning as the group continues to aggressively employ the latest technology as part of its nefarious strategy. ISIS' messaging effectively blends both officially endorsed and informal propaganda to recruit followers via numerous digital communication platforms. Due to many technological advances, the message of radicalization spreads faster than we imagined just a few years ago. Like never before, social media allows foreign terrorists to reach into our local communities — for the purpose of targeting our citizens to radicalize and recruit them.

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 is using 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 threats to the homeland.

Going Dark

Virtually every national security threat and criminal problem that the FBI currently faces has an element that is digitally-based or facilitated. Unfortunately, there is a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so. The FBI refers to this growing challenge as "Going Dark," and it affects the spectrum of our work. 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. Some of our criminal investigators face the challenge of identifying online pedophiles who hide their crimes and identities behind layers of anonymizing technologies, or drug traffickers who use virtual currencies to obscure their transactions. In other investigations, ranging from white collar crime to gang activity, FBI agents with court-ordered search warrants seize and attempt to search cellular phones, tablets, and other electronic devices, but are unable to access them due to technical barriers.

In just the first half of this fiscal year, the FBI was unable to access the content of more than 3,000 mobile devices using appropriate and available technical tools, even though there was legal authority to do so. This figure represents nearly half of all the mobile devices the FBI attempted to access in that timeframe.

Where at all possible, our agents develop investigative workarounds on a case-by-case basis, including by using physical world techniques and examining non-content sources of digital information (such as metadata). As an organization, the FBI also invests in alternative methods of lawful engineered access.

Ultimately, these efforts, while significant, have severe constraints. Non-content information, such as metadata, is often simply not sufficient to meet the rigorous constitutional burden to prove crimes beyond a reasonable doubt. Developing alternative technical methods is typically a time-consuming, expensive, and uncertain process. Even when possible, such methods are difficult to scale across investigations, and may be perishable due to a short technical lifecycle or as a consequence of disclosure through legal proceedings.

Some observers have conceived of this challenge as a tradeoff between privacy and security. In our view, the demanding requirements to obtain legal authority to access data—such as by applying to a court for a warrant or a wiretap — necessarily already account for both privacy and security. The FBI is actively engaged with relevant stakeholders, including companies providing technological services, to educate them on the corrosive effects of the Going Dark challenge on both public safety and the rule of law. The FBI thanks the committee members for their engagement on this crucial issue.

Intelligence

Integrating intelligence in all we do remains a critical strategic pillar of the FBI strategy. The constant evolution of the FBI's intelligence program will help us address the ever-changing threat environment. We must constantly update our intelligence apparatus to improve the way we use, collect, and share intelligence to better understand and defeat our adversaries. We cannot be content to only work the matters directly in front of us. We must also look beyond the horizon to understand the threats we face at home and abroad and how those threats may be connected.

To that end, we gather intelligence, consistent with our authorities, to help us understand and prioritize identified threats, to reveal the gaps in what we know about these threats, and to fill those gaps. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to organize threats into priorities for each of the FBI's 56 field offices. By categorizing threats in this way, we place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade to improve our understanding and mitigation of threats. Over the past few years, we have taken several steps to improve this integration. First, we

established an Intelligence Branch within the FBI, headed by an Executive Assistant Director who drives integration across the enterprise.

We also developed and implemented a series of integration-focused forums that ensure all members of our workforce understand and internalize the importance of intelligence integration. We now train our Special Agents and Intelligence Analysts together at the FBI Academy where they engage in joint training exercises and take core courses together prior to their field deployments. As a result, they are better prepared to integrate their skillsets in the field. Additionally, our training forums for executives and frontline supervisors continue ensure our leaders are informed about our latest intelligence capabilities and allow them to share best practices for achieving intelligence integration.

Counterintelligence

Our nation still confronts traditional espionage — spies posing as diplomats or ordinary citizens. But espionage has evolved; spies today are often students, researchers, or businesspeople operating front companies. And they seek not only state secrets, but trade secrets, research and development, intellectual property, and insider information from the Federal government, U.S. corporations, and American universities. Foreign intelligence entities continue to grow more creative and more sophisticated in their methods to steal innovative technology, critical research and development data, and intellectual property. Their efforts seek to erode America's leading edge in business, and pose a significant threat to our national security.

We remain focused on the growing scope of the insider threat — that is, when trusted employees and contractors use their legitimate access to information to steal secrets for the benefit of 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.

Weapons of Mass Destruction

The FBI, along with its U.S. government partners, is committed to countering the Weapons of Mass Destruction ("WMD") threat (*e.g.*, chemical, biological, radiological, nuclear) and preventing terrorist groups and lone offenders from acquiring these materials either domestically or internationally.

Domestically, the FBI's counter-WMD threat program, in collaboration with our U.S. government partners, prepares for and responds to WMD threats (*e.g.*, investigate, detect, search, locate, diagnostics, stabilization, and render safe WMD threats). Internationally, the FBI, in cooperation with our U.S. partners, provides investigative and technical assistance as well as capacity-building programs to enhance our foreign partners' ability to detect, investigate, and prosecute WMD threats.

One international success of our counter WMD threat program is our relationship with the Moldovan authorities who we have worked with closely to combat the nuclear smuggling threat for a number of years. In the spring of 2014, the FBI supported two joint investigations targeting WMD trafficking in Moldova. These operations targeted two separate networks that were smuggling allegedly radioactive material into Moldova. The operations resulted in arrests by Moldovan Police in December 2014 and February 2015. Depleted and natural uranium were seized in December 2014, and an unknown, liquid metal contained in an ampoule, purported to be cesium, was seized in February 2015.

Cyber

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. We face sophisticated cyber threats from state-sponsored hackers, multi-national cyber syndicates, purveyors of ransomware, hacktivists, and terrorists. On a daily basis, cyber-based actors seek to target our critical infrastructure and to harm our national security and economy. As we continue to see an increase in the scale and scope of reporting of 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, the FBI has actively coordinated with our private and public partners to pierce the veil of anonymity surrounding cyber-based crimes.

One example of the FBI's success in this area is the indictment of four individuals in connection with a data breach of more than 500 million Yahoo accounts. Beginning in January 2014, these individuals directed and took part in a cyber intrusion conspiracy. They then used the stolen information to obtain access to accounts at Yahoo, Google, and other providers. On February 28, 2017, charges were brought against Russian Federal Security Service officers Dmitry Dokuchaev and Igor Sushchin, as well as criminal hackers Alexey Belan and Karim Baratov. Given the complexity of this investigation, assistance and support from our international partners was essential in bringing these criminals to justice, as was collaboration with the victim companies, which highlights the value of proactive engagement and cooperation between the private sector and the government.

Given that malicious cyber-activity is not limited to one location, the FBI has worked to address this evolving threat through the Cyber Assistant Legal Attaché ("Cyber ALAT") program. This program embeds cyber agents, who are trained both at FBI Headquarters and in the field, with our international counterparts in 19 strategic locations across the globe where they build relationships with our international partners. These relationships are essential to working cyber cases which often involve malicious actors using computer networks worldwide.

Criminal

We face many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent

crime and public corruption. Criminal organizations — domestic and international — and individual criminal activity represent a significant threat to our security and safety in communities across the Nation.

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 State, local, and tribal officers and deputies on joint task forces and individual investigations.

FBI joint task forces — Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces — focus on identifying and targeting major groups operating as criminal enterprises. Much of the FBI 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.

In March of this year, the Attorney General issued a memorandum directing Federal prosecutors to focus on violent crime offenders. To support this effort, he also established a Task Force on Crime Reduction and Public Safety composed of Department of Justice ("the Department") representatives, including all four Department law enforcement agencies. These representatives are being tasked with making recommendations to the Attorney General on ways in which the Federal government can most effectively combat violent crime. The FBI is committed to working with the Department to bring violent offenders to justice.

Transnational Organized Crime

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

FBI continues to share intelligence about criminal groups with our partners and to combine resources and expertise to gain a full understanding of each group.

Crimes Against Children

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

The FBI also has several programs in place to educate both parents and children about the dangers posed by predators and to recover missing and endangered children should they be taken. Through our Child Abduction Rapid Deployment Teams, Innocence Lost National Initiative, Innocent Images National Initiative, annual Operation Cross Country, Office for Victim Assistance, 74 Child Exploitation Task Forces, and numerous community outreach programs, the FBI and its partners are working to keep our children safe from harm.

Operation Cross Country, a nationwide law enforcement action focusing on underage victims of prostitution, completed its tenth iteration during October 2016. Over 300 operational teams from 400 agencies across 135 cities and 55 FBI Field Offices were instrumental in recovering 82 child victims. Also arrested were 239 traffickers and associates and 996 adult prostitution subjects. One hundred and nine victim specialists, in coordination with local law enforcement victim advocates and non-governmental organizations, provided 327 direct services to the recovered victims. In addition to the services to recovered minors, 1,136 adults were provided outreach services during the operational period. From the first Operation Cross Country to this most recent action, 837 children have been recovered and 1,254 johns have been arrested.

Furthermore, the FBI established the Child Sex Tourism Initiative to employ proactive strategies to identify U.S. citizens who travel overseas to engage in illicit sexual conduct with children. These strategies include a multi-disciplinary approach through partnerships with foreign law enforcement and non-governmental organizations to provide child victims with available support services. One example of a Child Sex Tourism Initiative achievement is the conviction of Jason Jayavarman. In March 2015, Jayavarman, a dual Cambodian and U.S. citizen, received an 18-year Federal sentence within the United States, and was convicted of attempted sexual exploitation of a child for the purpose of producing child pornography, and of attempted travel with the attempt to aid and abet others in illicit sexual conduct in a foreign place.

Similarly, the FBI's Innocence Lost National Initiative serves as the model for the partnership between Federal, State, local, and international law enforcement partners in addressing child prostitution. Since its inception, more than 6,390 children have been located

and recovered. The investigations and subsequent 2,622 convictions have resulted in lengthy sentences, including 28 life terms.

Public Corruption

The Public corruption threat — which involves the corruption of local, State, and federally elected, appointed, or contracted officials — strikes at the heart of government, eroding public confidence and undermining the strength of our democracy. It affects how well U.S. borders are secured and neighborhoods are protected, how verdicts are handed down in court, and how well public infrastructure such as schools and roads are built. The FBI is uniquely situated to address this threat with our ability to conduct undercover operations, perform electronic surveillance, and run complex cases. However, partnerships are critical and we work closely with Federal, State, local, and tribal authorities in pursuing these cases.

One key focus is border corruption. The Federal government protects 7,000 miles of U.S. land border and 95,000 miles of shoreline. Every day, more than a million visitors enter the country through one of the 328 official Ports of Entry along the Mexican and Canadian borders, as well as through seaports and international airports. Any corruption at the border enables a wide range of illegal activities along these borders, potentially placing the entire nation at risk by letting drugs, guns, money, and weapons of mass destruction slip into the country, along with criminals, terrorists, and spies. Another focal point concerns election crime. Although individual States have primary responsibility for conducting fair and impartial elections, the FBI becomes involved when paramount Federal interests are affected or electoral abuse occurs.

Health Care Fraud

In 2016, the United States' health care expenditures were $3.4 trillion. These large sums present an attractive target for criminals. Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, and every taxpayer who funds Medicare is a victim. Schemes can also cause actual patient harm, including subjecting patients to unnecessary treatment or providing substandard services and supplies. As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used appropriately and not to line the pockets of criminals.

The FBI currently has over 2,800 pending health care fraud investigations. Over 70 percent of these investigations involve government funded programs, including Medicare, Medicaid, Children's Health Insurance Program, Department of Veterans Affairs, and Department of Defense. As part of our collaboration efforts, the FBI maintains investigative and intelligence sharing partnerships with government agencies such as other components within the Department, the Department of Health and Human Services, the Food and Drug Administration, State Medicaid Fraud Control Units, and other State, local, and tribal agencies. On the private side, the FBI conducts significant information sharing and coordination efforts with private insurance partners, such as the National Health Care Anti-Fraud Association, the National Insurance Crime Bureau, and private insurance investigative units. The FBI is also actively

involved in the Health Care Fraud Prevention Partnership, an effort to exchange facts and information between the public and private sectors in order to reduce the prevalence of health care fraud.

Civil Rights

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

Crimes of hatred and prejudice are a sad fact of American history. When members of a family are attacked because of the color of their skin, their sexual orientation, or their religious beliefs — real or perceived—our nation is left at a loss. The FBI is committed to working with the Department to ensure the civil rights of all people are respected and protected. We will continue to work with our local, State, and Federal law enforcement partners to be certain that officers and agents have the resources and training they need.

We need to do a better job of tracking and reporting hate crime and "color of law" violations to fully understand what is happening in our communities and how to stop it. There are jurisdictions that fail to report hate crime statistics. Others claim there were no hate crimes in their community — a fact that would be welcome if true. We must continue to impress upon our State and local counterparts in every jurisdiction the need to track and report hate crimes and to do so accurately. It is not something we can ignore or sweep under the rug.

Need for Incident-Based Crime Data

The latest Uniform Crime Reporting statistics, the *Preliminary Semiannual Uniform Crime Report*, January-June, 2016, show that the number of violent crimes in the Nation increased when compared with data for 2015. Moreover, this year we are seeing an uptick of homicides in some cities. There are a number of theories about what could be causing this disturbing increase in murders in our nation's cities, but we simply do not know for sure.

We need more and better data related to officer-involved shootings and altercations with the citizens we serve, attacks against law enforcement officers, and criminal activity of all kinds. For decades, the Uniform Crime Reporting ("UCR") program has used information provided by law enforcement agencies to measure crime. While knowing the number of homicides, robberies, and other crimes from any given year is useful, the data is not timely, and it does not go far enough to help us determine how and why these crimes occurred, and what we can do to prevent them.

Demographic data regarding law enforcement uses of force is not consistently reported to us through our UCR program. We in the FBI track and publish the number of "justifiable homicides" by police officers. Such reporting by police departments across the country perhaps

lacks sufficient incentive, so not all departments participate. The result is that currently we cannot fully track incidents involving police uses of force. And while the *Law Enforcement Officers Killed and Assaulted* report tracks the number of officers killed in the line of duty, we do not have a firm grasp on the numbers of officers assaulted in the line of duty. We cannot address concerns about law enforcement uses of force if we do not know the circumstances surrounding such incidents. We can use this data to tell us where problems may exist, and to inform us on needed improvements concerning the way we police our communities. By improving the way we collect and analyze data, we will have a more comprehensive understanding of what our communities are experiencing.

On February 9, 2016, I concurred with a Criminal Justice Information Services Advisory Policy Board recommendation to transition the UCR Program to a National Incident-Based Reporting System ("NIBRS") data collection. Unfortunately, only a little more than one third of our State, local, and tribal partners currently submit data to the National Incident Based Reporting System ("NIBRS"). One of the fears of police chiefs and sheriffs across the country is that by submitting data to the NIBRS, they may see an increase in statistics on criminal activity. However, an increase in statistics is not the same thing as an actual increase in crime. It means we are more accurately reporting what is happening in our communities. We hope to resolve that issue by phasing in the NIBRS over the next few years, and overlapping it with the Summary Reporting System and helping local jurisdiction better understand and message the data gleaned from NIBRS reporting.

The NIBRS will not have an immediate effect on our nation's crime problems, and we know it will take more than just data or more policing to solve these problems. However, we will continue to work with our partners in law enforcement to ensure that we can implement the NIBRS to get the data we need to best serve our communities.

Five Eyes Law Enforcement Group

In August 2015, the FBI began its two-year term as the chair of the Five Eyes Law Enforcement Group ("FELEG"). The FELEG is an international coalition of law enforcement and intelligence agency leaders and subject matter experts from the Federal Bureau of Investigation; Drug Enforcement Administration; U.S. Immigration and Customs Enforcement, Homeland Security Investigations; the United Kingdom's National Crime Agency; the Royal Canadian Mounted Police; the Australian Federal Police; Australian Crime Commission; and New Zealand Police. The FELEG coordinates government international responses to global organized crime, money laundering, and cyber-based crime. Key goals of the FELEG are to improve the ability of partners to share intelligence and conduct joint law enforcement operations, while ensuring that they leverage one another's capabilities and benefit from shared learning and best practices.

FBI Laboratory

The FBI Laboratory is one of the largest and most comprehensive forensic laboratories in the world. Operating out of a state-of-the-art facility in Quantico, Virginia, and Huntsville,

Alabama, laboratory personnel travel the world on assignment, using science and technology to protect the Nation and support law enforcement, intelligence, military, and forensic science partners. The Lab's many services include providing expert testimony, mapping crime scenes, and conducting forensic exams of physical and hazardous evidence. Lab personnel possess expertise in many areas of forensics supporting law enforcement and intelligence purposes, including explosives, trace evidence, documents, chemistry, cryptography, DNA, facial reconstruction, fingerprints, firearms, and WMD.

One example of the Lab's key services and programs is the Combined DNA Index System ("CODIS"), which relies on computer technology to create a highly effective tool for solving crimes. It enables Federal, State, and local forensic labs to exchange and compare DNA profiles electronically, thereby connecting crimes to known offenders and other crimes. Another part of the National DNA Index System of CODIS, the National Missing Persons DNA Database, helps to identify missing and unidentified individuals.

The Terrorist Explosives Device Analytical Center ("TEDAC") is another example. TEDAC was formally established in 2004 to serve as the single interagency organization to receive, fully analyze, and exploit 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. Although originally focused on devices from Iraq and Afghanistan, TEDAC now receives and analyzes devices from all over the world.

The National Institute of Justice ("NIJ") and the FBI have formed a partnership to address one of the most difficult and complex issues facing our nation's criminal justice system: unsubmitted sexual assault kits ("SAKs"). The FBI is the testing laboratory for the SAKs that law enforcement agencies and public forensic laboratories nationwide submit for DNA analysis. The NIJ coordinates the submission of kits to the FBI, and is responsible for the collection and analysis of the SAK data. The goal of the project is to better understand the issues concerning the handling of SAKs for both law enforcement and forensic laboratories, and to suggest ways to improve the collection and processing of quality DNA evidence.

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 Lab 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 in Chattanooga, the church in Charleston, at the Census Bureau and NSA, the shooting death of a Pennsylvania State Trooper, the Metcalf Power Plant in San Francisco, the Boston Bombing/Watertown Boat scene, San Bernardino, and the Pulse nightclub in Orlando.

Information Technology

The Information and Technology Branch provides information technology ("IT") to the FBI enterprise in an environment that is consistent with intelligence and law enforcement capabilities, and ensures reliability and accessibility by members at every location at any moment in time. Through its many projects and initiatives, it is expanding its information technology product offerings to better serve the operational needs of the agents and analysts and raising the level of services provided throughout the enterprise and with its counterparts in the law enforcement arena and Intelligence Community.

FBI special agents and analysts must have the best technology tools available to be responsive to the advanced and evolving threats facing this country. Enterprise IT must be designed to provide the right information quickly to its employees. Likewise, IT equipment must be reliable and as close to where the work is performed as possible. This decreases the time between information collection and dissemination.

Sentinel, the FBI's enterprise case management system, was deployed in 2012 and is continuing to evolve its core features to serve the agent and analyst workforce worldwide. Driven by an agile rapid deployment model, Sentinel delivers new capabilities each month. Sentinel's major deliveries have consolidated systems, reduced administrative workload, and provided solutions to emergent mission needs for every branch of the FBI.

Finally, as part of the Federal mandate to decrease the number of data centers, the FBI is working with the Department to meet requirements and close 37 data centers in the next five years. As part of this effort, the FBI will expand its data centers in Pocatello, Idaho, and Clarksburg, West Virginia, to serve as the primary data centers for all Department components. The Clarksburg data center's expansion is scheduled for completion in early 2018, while the construction contract for the Pocatello facility was awarded in February 2017. The FBI's Cloud First initiative also will affect data center consolidation by redirecting approved systems to commercial cloud facilities and minimizing the capital investments made for on-premises hardware.

Conclusion

Chairman Grassley, Ranking Member Feinstein, and members of the committee, thank you again for this opportunity to discuss the FBI's programs and priorities. Mr. Chairman, we are grateful for the leadership that you and this committee have provided to the FBI. We would not be in the position we are today without your support. Your support of our workforce, our technology, and our infrastructure make a difference every day at FBI offices in the United States and around the world, and we thank you for that support.

I look forward to answering any questions you may have.