Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

FOR A HEARING CONCERNING
OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

PRESENTED
SEPTEMBER 28, 2016

Statement of
James B. Comey
Director
Federal Bureau of Investigation

Before the
Committee on the Judiciary
U.S. House of Representatives

For a Hearing Concerning
Oversight of the FBI

September 28, 2016

Good morning Chairman Goodlatte, Ranking Member Conyers, 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 threat-focused, intelligence-driven organization. Each FBI employee understands that to defeat the key threats facing our nation, we must constantly strive to be more efficient 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.

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

National Security

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. Threats of terrorism against the United States remains persistent and acute. The dangers posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists are extremely dynamic. The tragic events we witnessed last week in New York and New Jersey and last June in Orlando are a somber reminder that the challenges we face are not just foreign in nature – they also come from within our own borders. Our work is very difficult; we are looking for needles in a nationwide haystack, but we are also called upon to

figure out which pieces of hay might someday become needles. That is hard work and the particular challenge of identifying homegrown violent extremists.

Threats of terrorism remain our highest priority and create the most serious challenges for the FBI, the U.S. Intelligence Community, and our foreign, state, and local allies. ISIL is relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. In addition, we are confronting an explosion of terrorist propaganda and training materials available via the Internet and social media. As a result of online recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the U.S. to recruit and carry out acts. Terrorists in ungoverned spaces—both physical and cyber—readily disseminate poisoned propaganda and training materials to attract easily influenced individuals around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change and transformation from the terrorist threat our nation faced a decade ago.

ISIL's widespread reach through the Internet and social media is alarming as the group has proven dangerously competent at employing such tools for its nefarious strategy. ISIL uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Recently released propaganda has included various English language publications circulated via social media.

Social media also helps groups such as ISIL to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable persons of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging. Echoing other terrorist groups, ISIL has advocated for lone offender attacks in Western countries. Recent ISIL videos and propaganda specifically advocate for attacks against soldiers, law enforcement, and intelligence community personnel. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

Investigating and prosecuting ISIL offenders is a core responsibility and priority of the Department of Justice and the FBI. The Department has worked hard to stay ahead of changing national security threats and changing technology. The benefits of our increasingly digital lives,

however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage.
For instance, some of these conversations among ISIL supporters and sympathizers occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters. Similarly, 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. The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. If we cannot access this evidence, it will have ongoing, significant effects on our ability to identify, stop, and prosecute these offenders.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old- fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States, including both physical and electronic surveillance. Physical surveillance is a critical and essential tool in detecting, disrupting, and preventing acts of terrorism, as well as gathering intelligence on those who are capable of doing harm to the nation. Along with our domestic and foreign partners, we are collecting and analyzing intelligence about the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing; in partnership with our many federal, state, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public.

Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the homeland. However, when changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. Ultimately, we must ensure both the fundamental right of people to engage in private communications as well as the protection of the public.

Going Dark

While some of the contacts between groups like ISIL and potential recruits occur in publicly accessible social networking sites, others take place via encrypted private messaging platforms. This real and growing gap, which the FBI refers to as "Going Dark," is an area of continuing focus for the FBI; we believe it must be addressed, since the resulting risks are grave both in both traditional criminal matters as well as in national security matters.

The United States government actively communicates with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. Though the Administration has decided not to seek a legislative remedy at this time, we will continue the conversations we are having with private industry, State, local, and tribal law enforcement, our foreign partners, and the American people. The FBI thanks the committee members for their engagement on this crucial issue.

Intelligence

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken two steps to improve this integration. First, we have established an Intelligence Branch within the FBI headed by an Executive Assistant Director ("EAD"). The EAD looks across the entire enterprise and drives integration. Second, we now have Special Agents and new Intelligence Analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better prepared to work well together in the field. Our goal every day is to get better at using, collecting and sharing intelligence to better understand and defeat our adversaries.

The FBI cannot be content to just work with what is directly in front of us. We must also be able to understand the threats we face at home and abroad and how those threats may be connected. Towards that end, the FBI gathers intelligence, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps in what we know about these threats. We then seek to fill those gaps and learn as much as we can about the threats we are addressing and others on the threat landscape. 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 priority for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

Counterintelligence

We still confront traditional espionage—spies posing as diplomats or ordinary citizens. But espionage also has evolved. Spies today are often students, researchers, or businesspeople operating front companies. And they seek not only state secrets, but trade secrets, 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.

To combat this threat, the FBI's Counterintelligence Division has undertaken several initiatives. We directed the development, deployment, and operation of 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, multiple FBI divisions, and the private sector.

The Counterintelligence and Cyber Divisions have also partnered to create the Cyber-Counterintelligence Coordination Section. This goal of this section is to effectively identify, pursue, and defeat hostile intelligence services that use cyber means to penetrate or disrupt U.S. government entities or economic interests by increasing collaboration, coordination, and interaction between the divisions. Finally, the Counterintelligence Division and the Office of Public Affairs collaborated to conduct a joint media campaign regarding the threat of economic espionage. As a result of this collaboration, the FBI publicly released a threat awareness video called *The Company Man: Protecting America's Secrets*. This video is available on the FBI's public website and has been shown more than 1,300 times across the United States by the Counterintelligence Division's Strategic Partnership Coordinators to raise awareness and generate referrals from the private sector. The video was also uploaded to YouTube in July 2015 and has received over 97,000 views since then.

Cyber

We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber actors seek our state and 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. These threats seek to strike our critical infrastructure and to harm our economy.

The pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber-attacks as a top priority. Within the FBI, we are targeting the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets. We need to be able to move from reacting to such attacks after the fact to operationally preventing such attacks. That is a significant challenge, but one we embrace. 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. For example, as the committee is aware, the Office of Personnel Management (OPM) discovered last year that a number of its systems were compromised. These systems included those that contain information

related to the background investigations of current, former, and prospective federal government employees and contractors, as well as other individuals for whom a federal background investigation was conducted. The FBI is continuing to investigate this matter with our interagency partners to investigate this matter.

Another growing threat to businesses and individuals alike is Ransomware. Last year alone there was a reported loss of more than $24 million. The FBI works closely with the private sector so that companies may make informed decisions in response to malware attacks. Companies can prevent and mitigate malware infection by utilizing appropriate back-up and malware detection and prevention systems, and training employees to be skeptical of emails, attachments, and websites they don't recognize. The FBI does not condone payment of ransom, as such a payment does not guarantee a victim will regain access to their data, will not be targeted again, and may inadvertently encourage continued criminal activity.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and sharing inside and outside of government, to our internal emphasis on developing and retaining new talent and changing the way we operate to evolve with the cyber threat. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Criminal

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.

Public Corruption

Public corruption is the FBI's top criminal priority. The threat—which involves the corruption of local, state, and federally elected, appointed, or contracted officials—strikes at the heart of government, eroding public confidence and undermining the strength of our democracy. It affects how well U.S. borders are secured and neighborhoods are protected, how verdicts are handed down in court, and how well public infrastructure such as schools and roads are built. The FBI is uniquely situated to address this issue, 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 327 official Ports of Entry along the Mexican and Canadian borders, as well as through seaports and international airports. Any corruption at the border enables a wide range of illegal activities along these borders, potentially placing the entire nation at risk by letting drugs, guns, money, and weapons of mass destruction slip into the country, along with criminals,

terrorists, and spies. FBI-led Border Corruption Task Forces are the cornerstone of our efforts to root out this kind of corruption. Located in nearly two dozen cities along our borders, these task forces generally consist of representatives from the FBI; the Department of Homeland Security Office of Inspector General; Customs and Border Protection Internal Affairs; Transportation Security Administration; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms, and Explosives; U.S. Immigration and Customs Enforcement-Office of Professional Responsibility; and state and local law enforcement. Another focus 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.

Civil Rights

The FBI remains dedicated to protecting the constitutional 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.

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. We cannot address issues about use of force and officer-involved shootings or why violent crime is up in some cities if we don't know the circumstances. Some jurisdictions fail to report hate crime statistics, while others claim there are no hate crimes in their community—a fact that would be welcome if true. We must continue to impress upon our state and local counterparts in every jurisdiction the need to track and report hate crimes.. And we need the information they report to be accurate, to be timely and to be accessible to everybody or it doesn't do much good. On the part of the FBI, we are pushing for a more modern system of collecting data on officer-involved incidents and violent crime at all levels. It's a large undertaking; it will take a few years to ensure that all of the databases functional, but we are going to get there.

Health Care Fraud

We have witnessed an increase in health care fraud in recent years, including Medicare/Medicaid fraud, pharmaceutical fraud, and illegal medical billing practices. Health care spending currently makes up about 18 percent of our nation's total economy. 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 2,783 pending health care fraud investigations. Over 70 percent of these investigations involve government sponsored health care programs to include Medicare, Medicaid, and TriCare, as well as other U.S. government funded programs. As part of our collaboration efforts, the FBI maintains investigative and intelligence sharing partnerships with government agencies such as other Department of Justice components, Department of Health and Human Services, the Food and Drug Administration, the Drug Enforcement 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.

Violent Crime

Violent crimes and illegal gang activities exact a high toll on individuals and communities. Today's gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit their illegal activities to single jurisdictions or communities. Because of its authority, the FBI is able to work across jurisdictional 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 law enforcement 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 Bureau's criminal intelligence is derived from our state, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

Despite these efforts, there is something deeply disturbing happening all across America. The latest Uniform Crime Reporting statistics gathered from the *Preliminary Semiannual Uniform Crime Report, January-June, 2015,* show that the number of violent crimes in the nation increased by 1.7 percent during the first six months of 2015 as compared with figures reported for the same time in 2014, and this year we are also seeing an uptick of homicides in some cities. The police chiefs in these cities report that the increase is almost entirely among young men of color, at crime scenes in neighborhoods where multiple guns are recovered. There are a number of theories about what could be causing this disturbing increase in murders in our nation's cities

and the FBI is working with our federal, state, and local partners to uncover the root causes of violence and tackle it at its infancy.

Transnational Organized Crime

More than a decade ago, the image of organized crime was of hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states, but organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion dollar schemes from start to finish. These criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identity theft, 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 Bureau 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 to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA, 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, 71 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 ninth iteration during the first full week of October. Over 300 operational teams from over 500 agencies across 135 cities and 53 FBI Field Offices were instrumental in recovering child victims of all races and arresting pimps and customers. Ninety victim specialists, in coordination with local law enforcement victim advocates and non-governmental organizations, provided services to child and adult victims.

Indian Country

There are 567 federally recognized tribes in the United States, with the FBI and the Bureau of Indian Affairs having concurrent jurisdiction for felony-level crimes on over 200 reservations.

According to the 2010 Census, there are nearly five million people living on over 56 million acres of Indian reservations and other tribal lands. Criminal jurisdiction in these areas of our country is a complex maze of tribal, state, federal, or concurrent jurisdiction.

The FBI's Indian Country program currently has 124 special agents in 34 FBI field offices primarily working Indian Country crime matters. The number of agents, the vast territory, the egregious nature of crime being investigated, and the high frequency of the violent crime handled by these agents makes their responsibility exceedingly arduous. The FBI has 15 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country, and we continue to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

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

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

FBI Laboratory

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

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

Another example of the laboratory's work is the Terrorist Explosives Device Analytical Center (TEDAC).. 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 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 in recent years include the shootings in Chattanooga, the Charleston church shooting, the shootings at the Census Bureau and NSA, the shooting death of a Pennsylvania State Trooper, the Metcalf Power Plant shooting in San Francisco, and the Boston Bombing/Watertown Boat scene.

Information Technology

The Information and Technology Branch provides information technology 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 (IT) 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 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, as close to where

the work is performed as possible. By doing so, the FBI will decrease the time between information collection and dissemination.

Special agents and intelligence analysts are most effective when their individual investigative and intelligence work and collected information is connected to the efforts of thousands of other agents and analysts. We have developed software that makes that possible by connecting cases to intelligence, threats, sources, and evidence with our enterprise case and threat management systems. Similarly, we have provided our agents and analysts with advanced data discovery, analytics, exploitation, and visualization capabilities through tools integration and software development. In addition, we have enterprise business applications that address administrative, legal compliance, internal training standards, investigative and intelligence needs, and information sharing services. These tools allow for better data sharing with our law enforcement partners and allow FBI agents and analysts to share FBI intelligence products with our Intelligence Community partners around the world.

Conclusion

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States from all of those threats and the men and women of the Bureau continue to meet and exceed those expectations, every day. I want to thank them for their dedication and their service.

Chairman Goodlatte, Ranking Member Conyers, 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.