Department of Justice

STATEMENT

OF

JAMES B. COMEY, JR.
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 ON

MAY 21, 2014

Statement of James B. Comey
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary
May 21, 2014

Good morning Chairman Leahy, Ranking Member Grassley, and members of the Committee. I look forward to discussing 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 it to maximum effect to carry out our mission.

Today's FBI is a threat-focused, intelligence-driven organization. Each employee of the FBI understands that to mitigate 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 facing our nation and our neighborhoods 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, 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

The FBI is the lead domestic intelligence and law enforcement agency in the United States. Our complementary intelligence and law enforcement capabilities make up the key components of the Bureau's national security mission. They also illustrate the unique authorities and mission we have in the U.S. Intelligence Community. We collect intelligence to understand and identify the threats to the nation. And when the time comes for action to prevent an attack, we disrupt threats using our law enforcement powers through our Joint Terrorism Task Forces (JTTFs).

Much of the FBI's success can be credited to the longstanding relationships we enjoy with our intelligence, law enforcement, public, and private sector partners. With thousands of private and public business alliances and more than 4,100 JTTF members, including more than 1,500 interagency personnel from more than 600 Federal, state, territorial, and tribal partner agencies, the FBI's partnerships are essential to achieving our mission and ensuring a coordinated approach toward national security threats.

Counterterrorism

As the lead agency responsible for countering terrorist threats to the United States and its interests overseas, the FBI integrates intelligence and operations to detect and disrupt terrorists and their organizations.

Counterterrorism remains our top priority and that isn't likely to change. Overseas, the terrorist threat is complex and ever changing. We are seeing more groups and individuals engaged in terrorism, a wider array of targets, greater cooperation among terrorist groups, and continued evolution in tactics and communication.

Al Qaeda core isn't the dominant force it once was, but it remains intent on causing death and destruction. Groups with ties to Al Qaeda continue to present a top threat to our friends and partners, and in some cases to the United States and our interests abroad. We also have citizens traveling overseas—especially to Syria—and radicalizing there, and then coming home. And they are traveling from all over the United States to all parts of the world.

As the Boston bombings illustrate, we face a continuing threat from homegrown violent extremists. This threat is of particular concern. These individuals are self-radicalizing. They do not share a typical profile; their experiences and motives are often distinct. They are willing to act alone, which makes them difficult to identify and stop. This is not just a D.C., New York, or Los Angeles phenomenon; it is agnostic as to place.

We also face domestic terrorism from individuals and groups who are motivated by political, racial, religious, or social ideology—ideology fueled by bigotry and prejudice—as we saw in Overland Park, Kansas.

We in the FBI have a strong working knowledge of these groups and their general membership. Here, too, it's the lone offenders that trouble us. They stand on the periphery. We may not know of them because their actions do not predicate an investigation. Most of the time, domestic extremists are careful to keep their actions within the bounds of constitutionally protected activity. And for the FBI, protecting those civil liberties—such as freedom of speech—is of paramount importance, no matter how hateful that speech might be. We only get involved when words cross the line into illegal activity.

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, research and development, intellectual property, and insider information from the federal government, U.S. corporations, and American universities. Foreign intelligence services continue to grow more creative and more sophisticated in their methods to steal innovative technology, critical research and development data, and intellectual property, which erodes America's leading edge in business and poses a significant threat to 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 educates academic and business partners about how to protect themselves against economic espionage. We also work with the defense industry, academic institutions, and the general public to address the increased targeting of unclassified trade secrets across all American industries and sectors. Together with our intelligence and law enforcement partners, we must continue to protect our trade secrets and our state secrets, and prevent the loss of sensitive American technology.

Weapons of Mass Destruction

As weapons of mass destruction (WMD) threats continue to evolve, the FBI uses its statutory authorities to lead all investigations concerning violations of WMD-related statutes, preparation, assessment, and responses to WMD threats and incidents within the United States. The FBI provides timely and relevant intelligence analyses of current and emerging WMD threats to inform decision makers, support investigations, and formulate effective countermeasures and tripwires to prevent attacks.

To ensure an effective national approach to preventing and responding to WMD threats, the FBI created the Weapons of Mass Destruction Directorate integrating the necessary counterterrorism, intelligence, counterintelligence, and scientific and technological components into one organizational structure. Using this integrated approach, the Directorate leads WMD policy development, planning, and response to ensure its efforts result in a comprehensive response capability that fuses investigative and technical information with intelligence to effectively resolve WMD threats.

To enable the prevention or disruption of WMD threats or attacks, FBI headquarters personnel, 56 field WMD coordinators, and two WMD assistant legal attachés oversee implementation of national and international initiatives and countermeasures. The FBI conducts outreach and liaison efforts with critical infrastructure partners, the private sector, academia, industry, and the scientific community to implement tripwires that prevent any actor – terrorist, criminal, insider threat, or lone offender – from successfully acquiring chemical, biological, radiological, or nuclear material or dissemination equipment. Through these efforts, the WMD Directorate supports the broader work of the U.S. government as a leading partner and active contributor to policy decisions.

The Counterproliferation Center (CPC) combines the operational activities of the Counterintelligence Division, the subject matter expertise of the WMDD, and the analytical capabilities of both components to identify and disrupt proliferation activities. Since its inception in July 2011, the CPC has overseen the arrest of approximately 65 individuals, including several considered by the U.S. Intelligence Community to be major proliferators. Along with these

arrests, the CPC has increased its operational tempo to collect valuable intelligence on proliferation networks.

Intelligence

The FBI's efforts to advance its intelligence capabilities have focused on streamlining and optimizing the organization's intelligence components while simultaneously positioning the Bureau to carry out its responsibilities as the lead domestic intelligence agency.

One way the FBI is enhancing our partnerships and our ability to address threats is through the Domestic Director of National Intelligence (DNI) Representative Program. Through this program, FBI senior-level field executives in 12 geographic locations are serving as DNI representatives throughout the United States. The Domestic DNI Representatives are working with Intelligence Community partners within their regions to understand the threat picture and develop a more coordinated and integrated Intelligence Community enterprise. A more unified and effective Intelligence Community will enhance the nation's ability to share information with our law enforcement and private sector partners, and will prevent and minimize threats to our national security.

In addition, we expanded the fusion cell model, which further integrates our intelligence and operational elements through teams of analysts embedded with agents in the operational divisions. These fusion cells examine the national and international picture and provide intelligence on current and emerging threats across programs, making connections that are not always visible at the field level. Providing standard criteria, these cells inform the Threat Review and Prioritization (TRP) process and develop National Threat Priorities for the field. The fusion cells assess the FBI's ability to collect intelligence to identify gaps, inform operational strategies, and mitigate threats to drive FBI operations. As a result, the fusion cells and TRP provide the field with clear guidance and a consistent process to identify priority threats, while ensuring FBI Headquarters has an effective way to manage and evaluate the most significant threats facing the country.

This strategic, national-level perspective ensures the FBI is developing a complete picture of the threat environment and directing our resources at priority targets to stay ahead of our adversaries. This integration provides a cross-programmatic view of current threats and enables a nimble approach to identifying and addressing emerging threats.

Cyber

We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas – things of incredible value to all of us. They may seek to strike our critical infrastructure and our economy. The threat is so dire that cyber security has topped the Director of National Intelligence list of global threats for the second consecutive year.

Given the scope of the cyber threat, agencies across the federal government are making cyber security a top priority. Within the FBI, we are targeting high-level intrusions – the biggest

and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We want to predict and prevent attacks, rather than reacting after the fact.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques – such as sources and wires, surveillance, and forensics – to fight cyber crime. We are working side-by-side with our federal, state, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24-hour cyber command center, CyWatch, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We also work with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance. And we are training our state and local counterparts to triage local cyber matters, so that we can focus on national security issues.

Our legal attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting partners at Interpol and The Hague as they work to establish international cyber crime centers. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe.

Cyber threats to critical infrastructure require a layered approach to cybersecurity, including partnerships with private sector owners and operators, and with Federal partners including the Department of Homeland Security (DHS). We have been successful in a joint campaign to combat a campaign of cyber intrusions targeting natural gas pipeline sector companies, in which the FBI and DHS's Industrial Control Systems -CERTCyber Emergency Response Team deployed onsite assistance to some of the organizations targeted, and provided 14 briefings in major cities throughout the United States to over 750 personnel involved in the protection of energy assets and critical infrastructure.

We have also successfully worked with DHS in to empower the US banking system to better defend against cyber attacks. As powerful distributed denial of service (DDoS) incidents impacting leading U.S. banking institutions in 2012 have persisted through 2014, the FBI has worked with DHS' US-CERT United States Computer Emergency Readiness Team to identify 600,000 DDoS-related IP addresses and contextual information, to better equip banks to defend themselves.

We know that to be successful in the fight against cyber crime, we must continue to recruit, develop, and retain a highly skilled workforce. To that end, we have developed a number of creative staffing programs and collaborative private industry partnerships to ensure that over the long term we remain focused on our most vital resource – our people.

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 impacts 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 and local 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 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, 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 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 cherished freedoms of all Americans. That 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—from lynchings to cross burnings to vandalism of synagogues—are a sad fact of American history. When members of a family are attacked because of the color of their skin, it's not just the family that feels violated, but every resident of that neighborhood. When a teenager is murdered because he is gay, the entire community feels a sense of helplessness and despair. And when innocent people are shot at random because of their religious beliefs—real or perceived—our nation is left at a loss.Stories like this are heartbreaking. They leave each one of us with a pain in our chest. Hate crime has decreased in neighborhoods across the country, but the national numbers remain sobering.

We need to do a better job of tracking and reporting hate crime to fully understand what is happening in our communities and how to stop it. There are jurisdictions that fail to report hate crime statistics. Other jurisdictions 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 crime and to do so accurately. It is not something we can ignore or sweep under the rug.

Financial Fraud Crimes

We have witnessed an increase in financial fraud in recent years, including mortgage fraud, health care fraud, and securities fraud.

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. With the economy and housing market still recovering in many areas, we have seen an increase in schemes aimed both at distressed homeowners and at lenders. Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud. We also work closely with the Department of Housing and Urban Development, Postal Inspectors, the IRS, the FDIC, and the Secret Service, as well as with state and local law enforcement offices.

Health care spending currently makes up about 18 percent of our nation's total economy. These large sums present an attractive target for criminals – so much so that we lose tens of billions of dollars each year to health care fraud. 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, every taxpayer who funds Medicare, is a victim. Schemes can cause actual patient harm, including subjecting patients to unnecessary treatment, providing substandard services and supplies, and by passing potentially life-threatening diseases due to the lack of proper precautions. As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used to care for the sick – not to line the pockets of criminals.

Our investigations of corporate and securities fraud have also increased substantially in recent years. As financial crimes become more sophisticated, so must the FBI. The FBI continues to use techniques such as undercover operations and Title III intercepts to address these criminal threats. These techniques are widely known for their successful use against organized crime, and they remain a vital tool to gain concrete evidence against individuals conducting crimes of this nature on a national level.

Finally, the FBI recognizes the need for increased cooperation with our regulatory counterparts. Currently, we have embedded agents and analysts at the Securities and Exchange Commission and the Commodity Futures Trading Commission, which allows the FBI to work hand-in-hand with U.S. regulators to mitigate the corporate and securities fraud threat. Furthermore, these relationships enable the FBI to identify fraud trends more quickly, and to work with our operational and intelligence counterparts in the field to begin criminal investigations when deemed appropriate.

Violent Crime

Violent crimes and 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. 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 and local 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 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.

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 multinational, 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, 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 our 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, Office of Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to keep our children safe from harm.

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 also include a multi-disciplinary approach through partnerships with foreign law enforcement and non-governmental organizations to provide child victims with available support services. Similarly, the FBI's Innocence Lost National Initiative serves as the model for the partnership between federal, state and local law enforcement in addressing child prostitution. Since its inception, more than 3,100 children have been located and recovered. The investigations and subsequent 1,450 convictions have resulted in lengthy sentences, including twelve life terms.

Indian Country

The FBI continues to maintain primary federal law enforcement authority to investigate felony crimes on more than 200 Indian reservations nationwide. More than 100 Special Agents from 20 different field offices investigate these cases. In addition, the FBI has 14 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 investigations concern homicide, crimes against children, or felony assaults.

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.

Science & Technology

Laboratory Services

The FBI Laboratory ("the Lab") 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 blends forensic science and computer technology into 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.

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.

Additionally, FBI Evidence Response Teams (ERTs) are active in all 56 field offices and include more than 1,200 members. The FBI supports and enables evidence collection capabilities of field ERTs and law enforcement partners by providing forensic training, resources, and expertise. The FBI also has forward-deployed evidence response capabilities to respond to terrorist attacks and criminal incidents involving hazardous materials (chemical, biological, nuclear, and radiological) in concert with local officials and FBI WMD experts.

Operational Technology

Terrorists and criminals are increasingly adept at exploiting cutting-edge technologies to carry out or to mask their crimes. To counter current and emerging threats, the FBI actively deploys a wide range of technology-based tools, capabilities, and training that enable and enhance intelligence, national security, and law enforcement operations. In addition to developing state-of-the-art tools and techniques, the FBI also focuses on recruiting and hiring individuals who possess specialized skills and experience. These dedicated employees serve as technically trained agents, engineers, computer scientists, digital forensic examiners, electronics technicians, and other specialists. Collectively, these specialists enable lawful electronic surveillance, provide secure communications, decipher encrypted messages, reverse engineer malware, forensically examine digital evidence such as images and audio recordings, and much more.

By way of example, the National Domestic Communications Assistance Center (NDCAC) is designed to leverage and share the law enforcement community's collective technical knowledge, solutions, and resources to address the challenges posed by advancing communications services and technologies. The NDCAC also works on behalf of federal, state,

local, and tribal law enforcement agencies to strengthen law enforcement's relationships with the communications industry.

The FBI has also established 16 Regional Computer Forensic Laboratories (RCFLs) across the nation. RCFLs serve as one-stop, full-service forensics laboratories and training centers. All RCFL personnel in each of the 16 facilities across the country must earn FBI certification as digital forensics examiners and follow standardized evidence handling and operating procedures. RCFLs are staffed by federal, state, and local law enforcement personnel who examine digital evidence in support of all types of investigations – cases involving everything from child pornography and terrorism to violent crime and economic espionage.

Criminal Justice Information Services

The FBI Criminal Justice Information Services (CJIS) Division, located in Clarksburg, West Virginia, provides federal state, and local enforcement and other authorized users with timely access to criminal justice information through a number of programs, including the National Crime Information Center, the National Instant Criminal Background Checks System and the Uniform Crime Reporting program which in intended to generate a reliable set of crime statistics for use in law enforcement administration, operation, and management.

In addition, CJIS manages the Integrated Automated Fingerprint Identification System (IAFIS), which provides timely and accurate identification services by identifying individuals through name, date-of-birth, fingerprint image comparisons, or other descriptors, and provides criminal history records on individuals for law enforcement and civil purposes. IAFIS is designed to process criminal fingerprint submissions in two hours or less and civil submissions in 24 hours or less. In FY 2013, approximately 62.7 million fingerprint background checks were processed. The Next Generation Identification program advances the FBI's biometric identification and investigation services, providing new biometric functionality such as facial recognition, improved latent searches, and immediate responses related to the Repository for Individuals of Special Concern, a fingerprint index of wanted persons, sexual offender registry subjects, known or appropriately suspected terrorists, and other persons of special interest.

CJIS also manages the Law Enforcement National Data Exchange (N-DEx), a criminal justice information sharing network that allows law enforcement agencies to share law enforcement records from more than 4,500 agencies with nearly 140,000 criminal justice users. The N-DEx network contains more than 225 million searchable records (incident reports, arrest reports, booking data, etc.). It is projected that by the end of FY 2014, N-DEx information sharing will be available to law enforcement agencies representing almost 60 percent of the U.S. population.

Critical Incident Response Group

The Critical Incident Response Group (CIRG) is a "one stop shop" for responding rapidly to crisis situations worldwide. Its professionals are on call around the clock, ready to support FBI operations and federal, state, local, and international law enforcement partners in managing critical incidents and major investigations.

The National Center for the Analysis of Violent Crime (NCAVC) provides operational support to FBI agents and law enforcement personnel on complex and time-sensitive cases. The Behavioral Threat Assessment Center (BTAC) assesses the potential threat of violence posed by persons of concern and as reflected in threatening communications. Issues traditionally addressed by the BTAC include school and workplace attacks, threats against Members of Congress and public figures, and threatening communications.

The Violent Criminal Apprehension Program (ViCAP) is the national repository for violent crime cases – specifically those involving homicides, sexual assaults, missing persons, and unidentified human remains – helping to draw links between seemingly unconnected crimes. In 2008, the FBI launched the ViCAP Web National Crime Database, which is available to law enforcement agencies through the secure LEO website. Investigators can search ViCAP Web for nationwide cases similar to theirs and communicate with other U.S. law enforcement agencies to coordinate investigations based on these linkages. More than 5,000 federal, state, and local law enforcement agencies have contributed to the 85,000-case ViCAP national violent crime database.

Active Shooter Training

In the aftermath of the tragedy at Sandy Hook elementary school, the President announced the Now Is the Time initiative focused on protecting children and communities by reducing gun violence. A critical component of this initiative focuses on schools, institutions of higher education, and houses of worship. The FBI was assigned to lead law enforcement training to ensure coordination among agencies. To that end, we have trained more than 9,600 senior state, local, tribal, and campus law enforcement executives at conferences hosted by FBI field offices, and trained more than 6,300 first responders through tabletop exercises designed around facts similar to recent school shootings. To date, the FBI has provided our Advanced Law Enforcement Rapid Response Training course, an active shooter training program, to more than 1,400 officers from 613 agencies.

Tactical Operations & Crisis Response

CIRG has a range of tactical resources and programs that support and provide oversight to the FBI and its partners. For example, each FBI field office has a SWAT team that is equipped with a wide array of specialized weaponry and is trained to engage in hazardous operations such as barricaded subjects, high-risk arrest/search warrants, patrolling through adverse terrain, and – in some field offices – maritime interdictions. These teams include crisis negotiators who routinely respond to prison sieges, hostage takings, and kidnappings nationwide and provide assistance to state and local police negotiators. CIRG also manages the FBI Hostage Rescue Team – the U.S. government's non-military, full-time counterterrorist tactical team – which provides enhanced manpower, training, and resources to confront the most complex threats.

The Hazardous Devices School at Redstone Arsenal in Huntsville, Alabama, is the nation's only facility for training and certifying public safety bomb technicians to render safe hazardous devices. Managed by the FBI, the school has trained more than 20,000 state and local

first responders since it opened in 1971. A natural extension of this school can be found in the FBI's own 249 Special Agent bomb technicians, who provide training to local and state bomb squads and serve as the workforce for the FBI's explosives-related operations worldwide.

Victim Assistance

Through the Office for Victim Assistance (OVA), the FBI ensures that victims of crimes investigated by the FBI are afforded the opportunity to receive the services and notifications required by federal law and the Attorney General Guidelines on Victim and Witness Assistance. Among its many services, OVA provides on-scene help to crime victims, assesses and triages their needs, and helps victims identify and secure counseling, housing, medical attention, and legal and immigration assistance. When other resources are not available, OVA administers special Victims of Crime Act funds to meet victims' emergency needs, including reunification travel, crime scene cleanup, replacement clothing, and shipment of victims' remains.

Special services are provided to child victims. The Child Pornography Victim Assistance Program coordinates support and notification services for child victims of pornography and their guardians. The Forensic Child Interviewing Program ensures that investigative interviews of child victims and witnesses of federal crimes are tailored to the child's stage of development and minimize any additional trauma. Additionally, a detailed protocol was recently developed for providing support to families of abducted children and assisting with post-recovery reunification and follow-up services. OVA is partnering with the Criminal Investigative Division's Violent Crimes Against Children Section and other agencies and organizations to improve the response to and services for minor victims of sex trafficking.

The Terrorism and Special Jurisdiction Program provides emergency assistance to injured victims and families of American victims killed in terrorist attacks and serves as a permanent point of contact for terrorism victims. Victim Assistance Rapid Deployment Teams provide immediate, on-scene assistance to victims of domestic terrorism and mass violence, often at the request of local law enforcement agencies. These highly trained and experienced teams have responded to numerous mass casualty crimes since 2006, most recently to tragedies at Sandy Hook Elementary School, the Washington Navy Yard, and at the Boston Marathon.

Information Technology

The FBI's Information and Technology Branch (ITB) provides enterprise-wide IT products and services to more than 36,000 FBI employees, contractors, and task force members, including managing more than 114,000 workstations and 46 mission-critical systems.

The target of the ITB's current modernization efforts is to create the future FBI Information Environment. Technology provides a distinct advantage, allowing FBI users access to their critical data when, where, and how they need it. The FBI Information Environment will support development of new mission and business functionality within a defined and controlled IT framework. These modernization efforts will move the FBI toward an agile, responsive, and efficient services-based operating model, emphasizing reuse of enterprise services both to increase cost savings and to enhance the reliability of IT infrastructure and applications.

International Offices

One of the fundamental challenges of the 21st Century is stopping overseas threats from compromising the security of the United States. For this reason, the FBI maintains more than 80 offices overseas that cover more than 200 countries and territories. Though our successes have been many, the increase in crimes with an overseas nexus shows we must do more.

The FBI operates worldwide and continuously looks for opportunities in the Middle East, Africa, Eurasia, the Americas, and Asia to target emerging terrorist, cyber, and criminal threats. Staff have strong cross-programmatic skills and work side-by-side with sister agencies, host governments, and corporate partners to take on threats. By targeting terrorists and criminals on their home turf – before their plots take shape – the FBI can stop those who wish to harm the United States before they have the capability to do so.

Training

With the support of Congress, we have re-opened the FBI Academy for training of new agents and intelligence analysts. In FY 2014, the FBI plans to graduate approximately seven new groups totaling more than 300 new agent trainees by the end of the fiscal year and approximately 140 new intelligence analysts in three session of the Intelligence Basics Course.

The National Academy provides law enforcement executives and investigators from state and local law enforcement agencies worldwide with advanced leadership training. The National Academy has continued to trained more executives, adding to its total of more than 47,000 graduates to date.

The FBI provides leadership, intelligence, and law enforcement assistance to its international training partners through a variety of programs designed to establish and strengthen cooperation and liaison between the FBI and its overseas counterparts. Courses offered include organized crime cases, anti-gang strategies, terrorist crime scene investigations, and street survival techniques. The FBI also participates in the Department of States's International Law Enforcement Academy (ILEA) program, providing instruction on specialized law enforcement techniques as well as leadership training at academies in Budapest, Hungary; Bangkok, Thailand; Gaborone, Botswana; and San Salvador, El Salvador; as well as the Regional Training Center in Lima, Peru. The FBI has supported the Director position in the Budapest academy since its establishment in 1996.

The curriculums of these academies incorporate tenets and techniques developed at the FBI National Academy. To date, more than 50,000 students from 85 countries have received ILEA training, and the FBI has been a prominent contributor to the program.

Other key training programs include Leadership in Counterterrorism, which has trained more than 400 upper-level counterterrorism executives from state or national police agencies and chiefs or deputy chiefs of local agencies to date; the Domestic Security Executive Academy, which has trained more than 340 federal executives and Fortune 1,000 corporate security

executives; the Law Enforcement Executive Development Seminar (LEEDS), a two-week program designed for chief executive officers of the nation's mid-sized law enforcement agencies; and the National Executive Institute (NEI), a two-week executive training program that provides strategic leadership education and partnership opportunities for executives from the highest levels of the FBI and the largest U.S. and international law enforcement agencies.

Leadership Development

We created the Leadership Development Program (LDP) to help prepare FBI employees to lead before taking formal leadership positions, by providing relevant tools, courses, and developmental experiences needed for success. These efforts are fostering a Bureau-wide cultural shift toward promoting long-term individual development to better operate in quickly developing transitions and crises.

Since 2009, LDP has built a variety of integrated programs, including onboarding for both new employees and specific positions such as executives and senior managers, in-depth courses for both current and new supervisors and program managers, and a developmental program to prepare aspiring leaders before they are promoted. LDP's various programs were created by employees, for employees, and are designed to build upon one another over the course of an employee's career. They were originally benchmarked against successful models from our military, law enforcement, and intelligence partners, as well as private companies; as LDP has grown, other government agencies now reach out to benchmark against the FBI.

Conclusion

Responding to this complex and ever-changing threat environment is not new to the FBI. Chairman Leahy, Ranking Member Grassley and members of the Committee, I would like to close by thanking you for this opportunity to discuss the FBI's priorities. We are grateful for the leadership that you have provided to the FBI. We would not be in the position we are today without your support. Your commitment in 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.

# # #