Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

JUNE 19, 2013

Statement for the Record
Robert S. Mueller, III
Director
Federal Bureau of Investigation

Committee on the Judiciary
U.S. Senate

"Oversight of the Federal Bureau of Investigation"
June 19, 2013

Good morning, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

Today's FBI is a threat-driven, intelligence-led organization. We have built a workforce and leadership team that view continuing transformation as the means to keep the FBI focused on key threats to our nation.

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 to our communities.

Counterterrorism remains our top priority. As illustrated by the recent attacks in Boston, the terrorist threat against the United States remains very real.

Yet national security is not our sole focus – we remain committed to our criminal programs. In the economic arena, investment fraud, mortgage fraud, and health care fraud have undermined the world's financial systems and victimized investors, homeowners, and taxpayers.

At the same time, gang violence, violent crime, crimes against children, and transnational organized crime pose real threats in communities across the country.

These diverse threats facing our nation and our neighborhoods underscore the complexity and breadth of the FBI's mission. To do this, we in the Bureau are relying on our law enforcement and private sector partners more than ever before.

Yet regardless of the challenges we face, the FBI remains firmly committed to carrying out our mission while protecting the civil rights and civil liberties of the citizens we serve.

I look forward to working with this committee in these final months of my term to ensure that the FBI maintains the capabilities needed to address these diverse threats now and into the future.

Counterterrorism

Over the past two months, we have seen an extraordinary effort by law enforcement, intelligence, and public safety agencies to find and hold accountable those responsible for the Boston bombings.

I would like to thank those who have worked tirelessly in the pursuit of safety and justice. These collaborative efforts, along with the public's help, enabled us to identify the individuals who we believe are responsible for this attack. Our thoughts and prayers remain with the bombing victims – those who perished and those who are embarking on a long road to recovery.

As this case illustrates, we face a continuing threat from homegrown violent extremists. These individuals present unique challenges because they do not share a typical profile. Their experiences and motives are often distinct, but they are increasingly savvy and willing to act alone, which makes them difficult to identify and to stop.

In the past two years, we have seen homegrown extremists attempt to detonate IEDS or bombs at such high profile targets as the Federal Reserve Bank in New York, commercial establishments in downtown Chicago, the Pentagon, and the U.S. Capitol. Fortunately, these attempts, as well as many others, were thwarted. Yet the threat remains.

Overseas, the terrorist threat is similarly complex and ever-changing. We are seeing more groups and individuals engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication.

Al Qaeda and its affiliates, especially al Qaeda in the Arabian Peninsula (AQAP), continue to represent a top terrorist threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

In December 2011, Somali national Ahmed Abdulkadir Warsame pled guilty to nine counts of providing material support to AQAP and al Shabaab. A Joint Terrorism Task Force investigation found that Warsarme conspired to teach terrorists how to make bombs, provided explosives weapons and training to al Shabaab and arranged for al Shabaab leaders to obtain weapons from members of AQAP. Warsame faces up to life in prison.

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.

They continue to grow more creative and more sophisticated in their methods to steal innovative technology, eroding America's leading edge in business and posing threats to national security. In the past four years, the number of arrests related to economic espionage has doubled, indictments have increased four-fold, and convictions have risen six-fold.

The loss of critical research and development data, intellectual property, and insider information poses a significant threat to national security.

In March, Steve Liu, a Chinese national and former employee of a New Jersey defense contractor, was sentenced to more than five years in prison for stealing thousands of electronic files detailing the performance and design of guidance systems for missiles, rockets, and drones. Liu traveled to China and delivered presentations about the technology at several Chinese universities.

These cases illustrate the growing scope of the "insider threat" — 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 become more global and increasingly exposed to foreign intelligence organizations.

We in the FBI are working to combat this threat. The 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.

And we are focused on the possible proliferation of weapons of mass destruction. In July 2011, the FBI established the Counterproliferation Center to identify and disrupt proliferation activities. The center combines the operational activities of the Counterintelligence Division, the subject matter expertise of the WMD Directorate, and the analytical capabilities of the Directorate of Intelligence. Since its inception in July 2011, the Counterproliferation Center (CPC) has overseen the arrest of approximately 50 individuals, including several considered by the U.S. Intelligence Community to be major proliferators.

For example, Lu Futain pled guilty on November 18, 2011, to federal charges of selling sensitive microwave amplifiers to the People's Republic of China (PRC). Lu was sentenced to 15 months in prison and three years of supervised release on October 29, 2012. Lu founded Fushine Technology, a corporation based in Cupertino, California, which exported electronic components used in communications and radar equipment. In April 2004, Lu's firm exported a microwave amplifier to co-defendant Everjet Science and Technology Corporation, a PRC-based company also owned by Lu, without having obtained a license from the U.S. Department of Commerce.

Susan Yip, a Taiwanese citizen, was sentenced to two years in prison on October 24, 2012, for helping obtain sensitive military parts for Iran in violation of the Iranian trade embargo. In her guilty plea, Yip admitted to using her Taiwan and Hong Kong-based companies to carry out a fraudulent scheme to violate the Iranian Transaction Regulations, by acting as a

broker and conduit for the purchase of items in the United States for shipment to Iran. From October 2007 to June 2011, Yip and her fellow conspirators obtained, or attempted to obtain, more than 105,000 parts valued at approximately $2.6 million. Yip helped buy the parts without notifying U.S. suppliers that the parts were being shipped to Iran, and without obtaining the required U.S. Government licenses.

Together with our law enforcement and intelligence partners, we must continue to protect our trade secrets and our state secrets, and prevent the loss of sensitive American technology.

Cyber

The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas, threatening innovation. And as citizens, we are also increasingly vulnerable to losing our personal information.

That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.

We in the FBI have built up a substantial expertise to address cyber threats, both here at home and abroad.

We have cyber squads in each of our 56 field offices, with more than 1,000 specially trained agents, analysts, and forensic specialists. We have hired additional computer scientists. The FBI also has 63 Legal Attaché offices that cover the globe. Together with our international counterparts, we are sharing information and coordinating investigations. We have Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players in the cyber crime arena.

Here at home, the National Cyber Investigative Joint Task Force comprises 19 law enforcement, military, and intelligence agencies to coordinate cyber threat investigations. We in the FBI work closely with our partners in the NSA and DHS. We have different responsibilities, with different "lanes in the road," but we must all be on the same page in addressing cyber threats.

The leaders of the FBI, DHS, and NSA recently met to clarify the lanes in the road in cyber jurisdiction. Together, we agreed that the DOJ is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DHS' primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. DoD's role is to defend the nation, gather intelligence on foreign cyber threats, and to protect national security systems.

Although our agencies have different roles, we also understand that we must work together on every substantial intrusion, and to share information among the three of us. Notification of an intrusion to one agency will be notification to us all.

In addition, the private sector is a key player in cyber security.

Private sector companies are the primary victims of cyber intrusions. And they also possess the information, the expertise, and the knowledge to be an integral partner in reducing instances of cyber crime.

In February 2013, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing.

One example of an effective public-private partnership is the National Cyber Forensics and Training Alliance – a proven model for sharing private sector information in collaboration with law enforcement. Located in Pittsburgh, the Alliance includes more than 80 industry partners from a range of sectors, including financial services, telecommunications, retail and manufacturing. The members of the Alliance work together with federal and international partners to provide real-time threat intelligence, every day.

Another initiative, the Enduring Security Framework, includes top leaders from the private sector and the federal government. This partnership illustrates that the way forward on cyber security is not just about sharing information, but also about solving problems – together.

We intend to further strengthen the bridges we have built between the federal government and the private sector in the cyber security realm. We must fuse private-sector information with information from the Intelligence Community and develop channels for sharing information and intelligence quickly and effectively.

Our success in resolving cyber investigations rests on the creative use of investigative techniques we have used throughout the FBI's history – physical surveillance, forensics, cooperating witnesses, sources, and court-ordered wire intercepts.

One example concerns the hacker known as "Sabu" – one of the co-founders of the hacktivist group LulzSec.

The case began when our Los Angeles Division collected numerous IP addresses used to hack into the database of a TV game show. Our New York Office used a combination of investigative techniques, including human sources, search warrants, and surveillance, to identify and locate Sabu.

We went to arrest him, and we gave him a choice: go to jail now, or cooperate.

Sabu agreed to cooperate, and he became a source, continuing to use his online identity. His cooperation helped us to build cases that led to the arrest of six other hackers linked to

groups such as Anonymous and LulzSec. It also allowed us to identify hundreds of security vulnerabilities – which helped us to stop future attacks, and limit harm from prior intrusions.

Defeating today's complex cyber threats requires us to continually evolve and adapt.

Instead of just building better defenses, we must also build better relationships. And we must overcome the obstacles that prevent us from sharing information and, most importantly, collaborating.

U.S. law enforcement and the Intelligence Community, along with our international and private sector partners, are making progress. However, technological advancements and expansion of the Internet continue to provide malicious cyber actors the opportunity to harm U.S. national security and the economy. Given the consequences of such attacks, the FBI must keep pace with this rapidly developing and diverse threat.

Criminal

With regard to criminal threats, our responsibilities range from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises, and from violent crime to public corruption. These criminal threats pose a significant threat to the safety and security of our communities.

Public Corruption

Public corruption is the FBI's top criminal priority. We have had a number of successful investigations in this area in recent years, including a racketeering indictment handed down in April. Twenty-five individuals, including 13 Maryland correctional officers, allegedly conspired with the Black Guerilla Family gang inside prisons to distribute drugs and launder money. Gang members allegedly bribed correctional officers at several Maryland prison facilities, convincing them to smuggle in drugs, cell phones, and other contraband. The correctional officers alerted imprisoned gang members of upcoming cell searches and several of the officers had long-term sexual relationships with the gang members and were impregnated by them. The defendants face maximum sentences of 20 years in prison.

Financial Crimes

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

Mortgage Fraud

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. As of May, the FBI had nearly 2,000 mortgage fraud investigations nationwide — and nearly three-fourths of these cases included losses of $1 million or more.

With the economy and housing market still recovering in many areas, we have seen an increase in schemes aimed at distressed homeowners, such as loan modification scams and phony foreclosure rescues.

Others seek to defraud lenders by submitting fraudulent loan documents and setting up straw buyers to purchase homes. The homes then go into foreclosure, the banks are left holding the bag, and neighborhoods are left to manage the blight associated with vacant properties.

Last month, the leader of a $66 million mortgage fraud scheme was sentenced to eight years in prison after arranging home sales between straw buyers and distressed homeowners. Gerard Canino, 51, from Long Island, New York, along with his co-conspirators, obtained mortgage loans for sham deals by submitting fraudulent applications to banks and lenders. The lenders sent the mortgage proceeds to the conspirators' attorneys and the attorneys submitted false statements to the lenders about how they were distributing the loan proceeds. They then distributed the loan proceeds among themselves and other members of their conspiracy.

Over the past five years, we have continued to boost the number of Special Agents investigating mortgage fraud. 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 Fraud

Health care spending currently makes up about 18 percent of our nation's total economy — and that percentage will continue to rise as our population ages. The federal government projects that by 2021, health care spending will reach 20 percent of the U.S. 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.

Last month, the Medicare Fraud Strike Force – a partnership between the Department of Justice and the Department of Health and Human Services – arrested 89 individuals, including doctors, nurses, and other licensed medical professionals, for allegedly participating in Medicare fraud schemes costing more than $223 million in false billing.

Since its inception in March 2007, Medicare Fraud Strike Force operations have charged more than 1,500 individuals who collectively have falsely billed the Medicare program for more than $5 billion.

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 sub-standard services and supplies, and 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.

Corporate and Securities Fraud

Another area where our investigations have increased substantially in recent years is in corporate and securities fraud. From September 2008 to April 2013, the FBI has seen a 36 percent increase in these cases, to more than 2,750 today.

One of our largest securities fraud cases centered on the Stanford Financial Group – a Houston, Texas, financial company that caused $7 billion in losses and impacted more than 30,000 victims. Using evidence obtained throughout the investigation, the FBI identified key executive management personnel who conspired to commit large-scale securities fraud. In January and February of 2013, the last of these co-conspirators were sentenced to prison. To date, five individuals have been sentenced, ranging from 3 years to 110 years in prison.

As financial crimes become more sophisticated, so must the FBI. In the post-financial crisis period, the FBI devoted an additional 150 Special Agents and more than 175 forensic accountants to combat evolving financial crimes.

In addition to the dedication of more personnel, the FBI continues to use sophisticated techniques, such as undercover operations and Title III intercepts, to address these criminal threats. These techniques have been 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.

Gangs/Violent Crime

For many cities and towns across the nation, violent crime – including gang activity – continues to pose a real and growing problem.

Gangs continue to become more sophisticated. They commit criminal activity, recruit new members in urban, suburban, and rural regions across the United States, and develop criminal associations that expand their influence over criminal enterprises, particularly street-level drug sales.

Gangs also have expanded their operations to alien smuggling, identity theft, and mortgage fraud. Our Violent Crime, Violent Gang/Safe Streets, and Safe Trails Task Forces target major groups operating as criminal enterprises – high-level groups engaged in patterns of racketeering. This allows us to identify senior leadership and to develop enterprise-based prosecutions.

Active Shooter Threats

Communities across America also continue to face active shooter and mass casualty incidents. Since the Sandy Hook tragedy last December, the FBI has been working with the Department of Justice's Bureau of Justice Assistance to provide tactical training to law enforcement agencies upon request.

One hundred FBI agents across the country have attended Advanced Law Enforcement Rapid Response Training (ALERRT) school and are prepared to train other officers in life-saving tactics. The 16-hour Basic Active-Shooter course prepares first responders to isolate any given threat, distract the threat actors, and end the threat. In addition, during the month of April, the FBI conducted two-day conferences and table top exercises with state, local, tribal, and campus law enforcement executives. We have also worked with experts at Texas State University to improve tactical training for officers that respond to active shooter situations and then held two-day conferences on active shooter situations at most of our 56 field offices nationwide. These conferences reached senior command staff from state, local, tribal and campus police agencies. These experiences gave behavioral experts, victim assistance specialists, and other personnel the opportunity to work through best practices and spurred discussions on how to best react to active shooter and mass casualty incidents. We are continuing our efforts with a new table top exercise specifically designed for campus law enforcement. This is an issue that impacts all of us, and the FBI is committed to working with our partners to protect our communities.

Transnational Organized Crime

We continue to confront organized crime. Crime syndicates run multi-national, multi-billion-dollar schemes – from human trafficking to health care fraud, and from computer intrusions to intellectual property theft.

These sophisticated enterprises come from every corner of the globe. Often they operate both overseas and in the United States, and include Italian, Russian, Asian, Balkan, Middle Eastern, and African syndicates as well as Outlaw Motorcycle Gangs. We work to cripple these national and transnational syndicates with every capability and tool we have: undercover operations; confidential sources; surveillance; intelligence analysis and sharing; forensic accounting; multi-agency investigations; and the power of racketeering statutes that help us take down entire enterprises. We also work closely with our international partners – in some cases, swapping personnel – to build cases and disrupt groups with global ties.

In the spring of 2012, four members of an Armenian organized crime ring were convicted in one of the largest bank fraud and identity theft schemes in California history. Two of those

convicted directed the scheme from behind bars. Using cell phones that were smuggled into a California state prison, they coordinated with others to obtain confidential bank profile information and stole money from high-value bank accounts. The six-year conspiracy cost more than $10 million in losses to victims throughout the Southwest.

Crimes Against Children

The FBI remains vigilant in its efforts to keep children safe and to find and stop child predators. Our mission is threefold – first to decrease the vulnerability of children to sexual exploitation through awareness; second, to provide a rapid and effective federal investigative response to crimes against children; and, third, to enhance and assist the capabilities of state and local law enforcement investigators through task force operations.

Through our entire Violent Crimes Against Children program, including the Child Abduction Rapid Deployment Teams, the Innocence Lost National Initiative, the Office of Victim Assistance, Innocent Images program, and numerous community outreach programs, the FBI and its partners are working to make the world a safer place for our children.

And as new technology and new tactics are used to lure our young people, we must evolve in our efforts to stop those who would do them harm.

In January, a 31-year-old man from Montgomery, Alabama, was sentenced to 35 years in prison for producing child pornography through a massive online sextortion scheme. Christopher Patrick Gunn reached out to hundreds of young girls, gained their trust and their personal information, and then threatened to reveal that information unless they sent sexually explicit images of themselves. Gunn victimized children in at least a half-dozen states and Ireland.

This case came to light after junior high school aged-victims contacted their local police in a small Alabama town. Authorities soon realized there were strikingly similar cases in Mississippi and Louisiana.

By combining our resources and using our partnerships with state, local, and international law enforcement, we are able to investigate crimes that cross geographical and jurisdictional boundaries.

In April, we apprehended Eric Justin Toth, who had been added to the FBI's Ten Most Wanted Fugitive list in April 2012, and is currently charged with production and possession of child pornography. Toth, who also used the name David Bussone, is a former camp counselor and private-school teacher who taught here in Washington, D.C. He had been on the run since 2008, after an FBI investigation revealed pornographic images on a camera in his possession while at the school where he taught. A recent tip led law enforcement to Nicaragua, where Toth was living under an alias. He was apprehended in Esteli, Nicaragua, and has been returned to the United States to face prosecution.

And in February, the FBI's Hostage Rescue Team, crisis negotiators, and behavioral analysts were instrumental in rescuing a five-year-old boy in Midland City, Alabama. Working with the Dale County Sheriff's Department and the Alabama Department of Public Safety, some 300 officers and agents worked side-by-side to end a six-day siege in which an anti-government gunman named Jimmy Lee Dykes killed Charles Poland, a heroic school bus driver who died protecting the children on his bus. Dykes kidnapped the boy and held him hostage in an underground bunker. For six days, local, state, and federal negotiators spoke with Dykes and attempted to resolve the situation peacefully. When it was clear Dykes was becoming more and more agitated, authorities feared that the boy was in imminent danger. At that point, members of the Hostage Rescue Team entered the bunker in an attempt to rescue the boy. Dykes immediately attempted to detonate one of several bombs he had planted around his property and fired several shots at law enforcement. Dykes died during the confrontation. The boy was rescued safely, and incredibly, no law enforcement officials were injured.

This case represents some of the finest collaboration between local, state, and federal law enforcement agencies in recent time.

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.

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.

Currently, the FBI has 14 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country. In addition, the FBI continues to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts.

We are using technology to improve the way we collect, analyze, and share information. In 2011, we debuted new technology for the FBI's Next Generation Identification System, which

enables us to process fingerprint transactions much faster and with more accuracy. We are also integrating isolated data sets throughout the Bureau, so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

Sentinel, the FBI's next-generation information and case management system was deployed to all employees on July 1, 2012. The system's indexing ability allows users to extract names, dates, vehicles, addresses, and other details, and to more efficiently share data with our law enforcement partners. Sentinel also enhances the FBI's ability to link cases with similar information through expanded search capabilities and to share new case information and intelligence more quickly among Special Agents and analysts.

The FBI shares information electronically with partners throughout the Intelligence Community, across the federal government, as well as with state and local agencies. For example, the FBI works closely with the nationwide Suspicious Activity Reporting (SAR) Initiative to ensure that SARs entered into the Justice Department's Information Sharing Environment's Shared Space system are simultaneously shared with eGuardian, the FBI's system used to collect and share terrorism-related activities among law enforcement, and in turn, delivered to the appropriate policing and Intelligence Community partners.

Going Dark

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

Court-approved surveillance is a vital tool for Federal, State, and local law enforcement authorities. It is, for example, critical in cyber cases where we are trying to identify those individuals responsible for attacks on networks, denial of service attacks, and attempts to compromise protected information. However, there is a growing gap between law enforcement's legal authority to conduct electronic surveillance, and its ability to conduct such surveillance. Because of this gap, law enforcement is increasingly unable to gain timely access to the information to which it is lawfully authorized and that it needs to protect public safety, bring criminals to justice, and keep America safe. We must ensure law enforcement capabilities keep pace with new threats and new technology, while at the same time protecting individual privacy rights and civil rights.

It is only by working together – within the law enforcement and intelligence communities, with our private sector partners and with members of Congress – that we will find a long-term solution to this growing problem. In March, the FBI took one step toward improved collaboration and communication with the opening of the National Domestic Communications Assistance Center. The center will enable law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice.

Civil Rights / Civil Liberties / Rule of Law

Technology is one tool we use to stay a step ahead of criminals and terrorists. Yet as we in the FBI continue to evolve to keep pace with today's complex threat environment, our values must never change. The rule of law remains our guiding principle.

Every FBI employee takes an oath promising to uphold the rule of law and the United States Constitution. For the men and women of the FBI, this is our guiding principle. In my remarks to New Agents upon their graduation from the FBI Academy, I emphasize that it is not enough to catch the criminal; we must do so while upholding his civil rights. It is not enough to stop the terrorist; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights make all of us safer and stronger. In the end, we will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

Conclusion

Chairman Leahy and Ranking Member Grassley, I thank you for this opportunity to discuss the FBI's priorities. The transformation the FBI has achieved during my term would not have been possible without your support and the support of the American people. Your investments in our workforce, our technology, and our infrastructure make a difference every day at FBI offices throughout the United States and abroad, and we thank you for that support.

I look forward to any questions that you may have.