DECEMBER 9, 2015

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HOUSE OF REPRESENTATIVES, COMMITTEE ON THE JUDICIARY

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS

Senator Chuck Grassley R (IA) *[view pdf]*

Senator Patrick Leahy D (VT) *[view pdf]*

WITNESS TESTIMONY

The Honorable James B. Comey, Jr. *[view pdf]*
Director
Federal Bureau of Investigation
Washington, DC

AVAILABLE WEBCAST(S):*

[Full Hearing]

COMPILED FROM:

- *http://www.judiciary.senate.gov/meetings/oversight-of-the-federal-bureau-of-investigation-12-2015*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Prepared Statement of Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing on Oversight of the Federal Bureau of Investigation
Wednesday, December 9, 2015

Director Comey, welcome and thank you for being here today. The FBI's mission is to protect us from the most dangerous threats facing our nation. The deadly attacks in Paris last month, and in California last week, confirmed that radical Islamic terrorism continues to be such a threat, regardless of whether that's politically correct or convenient for President Obama.

ISIS is a determined enemy executing a plan to gain and hold territory, enrich itself, inspire followers worldwide, and launch deadly attacks against the West. And the American people are worried. Not just about terrorism. But about the President's inability or unwillingness to rally the country, lead our international partners, develop a credible strategy to destroy ISIS, and execute it. We are now paying the price for that weakness.

At almost every turn, events have proven the President wrong about ISIS. In August 2012, he drew a "red line," warning the Assad's regime not to use chemical weapons in Syria. But the President backed down after Assad gassed his own people, and ISIS blossomed in the chaos that followed. In January 2014, the President referred to ISIS as the "j.v.," or junior varsity. It promptly spent the next six months conquering territory across Syria and Iraq. In August of that same year, the President conceded that he didn't have a strategy to defeat ISIS. A year and a half later, he remains without a coherent one. Even former Secretary Clinton admitted the other day that we're not winning this fight.

The President has been hoping that ISIS will go away, because its existence doesn't fit his preferred political narrative. But hope is not a strategy. Hope is not a plan. Hope is not action.

And all the while, the drumbeat of attacks in the United States continued. In May, there was the attack on a convention center in Garland, Texas. In June, police were forced to shoot a knife-wielding ISIS supporter on the streets of Boston. In July, we had the attack on military facilities in Chattanooga, Tennessee.

Director Comey, as of October you reported that the FBI was engaged in approximately 900 active domestic investigations against suspected ISIS-inspired operatives and other radicalized extremists. And you estimated that approximately 250 Americans have left the U.S. and traveled to Syria to fight with ISIS, or tried to do so.

Nonetheless, in November, the President assured us that ISIS was "contained." But the very next day, it inflicted the deadliest Islamic terrorist attacks in Europe in over a decade, a coordinated assault across Paris that killed 130 and injured over 350. A few weeks later, in San Bernardino, two of its apparent supporters executed the deadliest such attacks on the homeland since September 11, 2001.

Unfortunately, President Obama has responded to this crisis by trying to divide us, deride us, and distract us. He is doubling down on his failed strategy.

After reports suggested that one of the Paris terrorists possessed a Syrian passport and had entered Europe as a refugee, many expressed concern about the procedures used to screen refugees coming to the United States from Syria. Director Comey, you expressed similar concerns in October. You warned that there are "gaps" in the information we have to vet people coming out of a war zone. And you warned that letting anyone come to the United States carries some risk. We can point to the brothers who bombed the Boston Marathon as an example of terrorists who were granted asylum here.

The President responded to the concerns expressed by many Americans by mocking them for being afraid of "widows and orphans."

But events continued to prove the President spectacularly wrong. As it turns out, women are radical Islamic terrorists, too, apparently to the President's surprise. We now know that Ms. Malik, one of the San Bernardino attackers, arrived in the United States on a fiancée visa. This is yet another example of the failure of the screening process for those entering the United States. Our government apparently didn't catch the false address in Pakistan she listed on her application or other possible signs that she was radicalized or an operative.

To top it all off, earlier this week we learned that the National Counterterrorism Center has identified individuals with ties to terrorists in Syria who are attempting to enter the United States through the refugee program. I guess that was one intelligence report the administration couldn't shade to fit its preferred conclusions.

Now, it always bears repeating that *Islam is not our enemy*. Radical Islamic terrorists are. The vast majority of Muslims in this country and around the world are non-violent and law-abiding. We all should oppose, in no uncertain terms, any violence or intimidation against Muslims for their practicing their religion. But I fear that one of the reasons for the regrettable backlash against Muslims in this country is the public's frustration with the President's repeated public failure to acknowledge the actual nature of the threat that we face, his reluctance to utter the words radical Islamic terrorism.

President Obama has also continued to divide us, deride us, and distract us with the issue of gun control. To the President, radical Islamic terrorism is never to blame. But the constitutional right to own a gun always is.

But terrorists aren't deterred by gun control. Strict European gun control laws did not stop the Paris attacks. California's assault weapons ban didn't stop the San Bernardino massacre.

Now, the Obama administration argues that allowing foreigners to buy guns who enter the United States through the visa waiver program is a problem. I agree. But at the same time, the administration's apparently fine with allowing refugees, asylees, people on deferred action, and other non-citizens who are not legal permanent residents to buy guns. This makes no sense. With few exceptions, we need to prevent all of these people from buying guns.

The administration's current fixation with guns and the visa waiver program can be explained, though, because it's another area where the administration's actions have made Americans less safe. In fact, an opinion from the Obama Justice Department required the Bureau of Alcohol, Tobacco, Firearms and Explosives to change its policy to permit persons arriving from visa waiver countries to buy guns. And the administration removed the longstanding requirement that non-citizens at least establish residency for 90 days in the state where they want to purchase a gun. These 90 days could be crucial in a terrorism investigation.

So when we address the issue of foreigners in the United States buying guns, we need to be comprehensive about it, not just clean up the mess this administration created.

Finally, the Democrats have attempted to divide us, deride us, and distract us with proposals to deny the right to purchase firearms to those on various terrorist watch lists, including the No Fly List.

The San Bernardino terrorists were apparently not on any terrorist watch list, so such a proposal wouldn't have stopped that attack. In addition, the President's claim that "people we don't allow to fly could go into a store right now in the United States and buy a firearm and there's nothing we can do to stop them" just isn't true. The FBI is notified when someone on the No Fly List attempts to purchase a gun, and can take steps to ensure that a gun doesn't fall into the wrong hands. So the President and others have been misleading the American people on that matter.

But the more fundamental point is this: while these lists are useful in keeping us safe, they are the result of the executive branch's unilateral decisions to put people on them without any notice or opportunity to be heard. As a result, they can be unreliable. And it just isn't constitutional to condition the fundamental right to keep and bear arms on an administrative list that lacks that kind of due process.

We wouldn't consider conditioning any other constitutional right – such as the freedoms of speech or religion, or from unreasonable searches and seizures – on such a process. That is why it is so surprising that this President, a former constitutional law professor, and so many Democrats, would support such a scheme.

The fact is, law enforcement hasn't raised gun purchases by people on terrorist watch lists as a huge problem. And Director Comey, I know that you know how to tell us when you confront a serious obstacle to keeping us safe. At our hearing in July, we all heard you talk about the "Going Dark" problem and the increasing use of encrypted communications by terrorists. After these most recent attacks, I'll be interested in hearing how your discussions with technology companies on that issue are proceeding.

I also look forward to discussing a range of other issues with you today. One is the FBI's treatment of whistleblowers. You've expressed a strong commitment to whistleblowers. During your confirmation hearing, you said that whistleblowers were "a critical element of a functioning democracy."

Our hearing in March this year showed that many FBI whistleblowers still have no protection, and the ones who are protected wait many years for relief. I hope that I have your support in strengthening the FBI whistleblower law.

In addition, in March 2015, the American people learned that Secretary Clinton used a private email address and non-government server during her time at the Department of State. Secretary Clinton unilaterally deleted approximately 30,000 emails without any government oversight. Her email and server arrangement is an example of Freedom of Information Act interference, a statute that is within this committee's jurisdiction. Concerns about the email arrangement extend beyond FOIA and involve national security.

And a former Department of State employee, Bryan Pagliano, has refused to communicate with this committee citing his Fifth Amendment right against self-incrimination.

Both the Department of Justice and FBI have refused to confirm or deny any investigation relating to Secretary Clinton's email arrangement citing "long standing policy." Yet, on a number of occasions, the department has publicly announced that it launched an investigation. The American people ought to know what their government is doing. I will have questions for you on this matter.

On another matter, in April, the Wall Street Journal reported that in 2012 the FBI helped facilitate a $250,000 ransom payment to al Qaeda from the family of kidnapped aid worker Warren Weinstein.

I wrote to the Department of Justice in May to ask if this was true. I also asked if the FBI had facilitated any other ransom payments to terrorist organizations. And I asked for more information about the FBI's policies and procedures relating to facilitating ransom payments to terrorist groups. I got a response letter five months later. That response did not really answer my questions.

Ransom payments are a significant source of terrorist financing. The FBI says its policy is quote "to deny hostage-takers the benefits of ransom" end quote. But the FBI also seems to say it may assist in private efforts to pay ransoms. So, it is not clear what is actually happening. It is not clear whether FBI has helped ransom payments get to terrorist groups.

In June, the Obama administration announced a new hostage recovery policy. It put the FBI in charge of an interagency Hostage Recovery Fusion Cell. Once again, it is unclear if the new hostage policy allows the FBI to facilitate ransom payments to terrorists. Some media outlets say that the new policy makes it easier to make these payments.

So, I'd like to get some specific answers about what the FBI does or does not do when it comes to ransom payments to terrorists. If it has helped with these payments, I'd like to know which terrorist groups received them and how much money they got.

Another issue I'll raise is the FBI's use of spyware. Six months ago, I wrote to the FBI to ask about its use of spyware. I still haven't received a response. According to press reports,

spyware is a type of software that can be remotely deployed to targeted computers and smart phones. Spyware can secretly activate the computer's camera and microphone; collect passwords; search the computer's memory; and intercept phone calls, text messages, and other communications. Spyware is a powerful surveillance tool. It has also been mentioned as a possible way to combat the "Going Dark" problem posed by encryption.

Tools like this need to be subject to oversight to make sure they are not abused. But the committee still does not know how the FBI is using these programs. We have asked. The FBI hasn't answered.

We don't know the types of spyware used or their capabilities. We don't know the FBI's policies and procedures for using spyware, or the legal processes used. And we don't know if there are any audit procedures in place to ensure spyware is used properly.

The Department of Justice is in the process of trying to change Rule 41 of the Rules of Criminal Procedure. The proposed change would make it easier for the FBI to get warrants to use spyware. Congress will eventually weigh in on the change. But we need to know more about spyware in order to make an informed decision.

So, I hope that I can get answers about the FBI's use of spyware. It is important for our oversight role, and it is important for the proposed change to Rule 41.

Finally, as you know, the FBI is conducting a review of federal and state criminal cases in which results of microscopic hair comparison analyses conducted in FBI Labs were used. The FBI has identified over 21,600 cases assigned to hair examiners prior to the year 2000. Cases since 2000 have had DNA analysis and so were not subject to the same potential problems that have led to the review.

Of those 21,600 cases, the FBI determined many of them did not have a microscopic hair analysis report sent to the requesting agency or there was not a conviction in the case. This left 3,118 cases where faulty lab work may have led to a criminal conviction.

The key step in evaluating those remaining 3,118 cases is getting and evaluating a trial transcript.

In a September 2015 letter, your staff said 689 of those cases have been closed because the FBI can't get an adequate response from case contributors or prosecutors. I will have a couple questions about those cases.

Again, thank you for being here, and I'll now recognize Ranking Member Leahy for his opening statement.

Statement Of Senator Patrick Leahy (D-Vt.),
Ranking Member, Senate Judiciary Committee
Hearing On Oversight Of The Federal Bureau Of Investigation
December 9, 2015

The Federal Bureau of Investigation is entrusted with the enormous responsibility of enforcing our laws and protecting the nation. No matter what the threat, and no matter what the motivation, the FBI is tasked with helping to keep us safe. On any given day, FBI agents around the country are investigating cases involving not only terrorism, but violent crime, gangs, cybercrime, identity theft, fraud, human trafficking, hate crimes, and child exploitation.

The events of the past six months have underscored the varied nature of the threats the FBI faces, and the key role it plays in protecting against terrorist acts. This past June, nine African American churchgoers were murdered by a white supremacist during a bible study in Charleston. The day after Thanksgiving, three individuals – including a police officer – were shot to death inside a women's health clinic in Colorado Springs. Last week, 14 county workers in San Bernardino were murdered in a shooting rampage. Director Comey may not be able to share all of the details about these investigations today, but I believe we can all agree that there is one common motivating factor behind each of these heinous crimes: hateful extremism.

These attacks remind us that we need to be vigilant against all forms of violent extremism. No one underestimates the incredibly difficult job of protecting the country from terrorist threats. So we have to support the law enforcement and intelligence officials who work to protect our nation by giving them the tools and resources they need to do their jobs effectively. And as we have heard from many law enforcement officials, we need to continue the hard work of building trust in our communities among neighbors, and with law enforcement, so that we can all share in the responsibility of keeping our communities safe.

At the same time, we must categorically reject the divisive and corrosive rhetoric of fear that only serves to undermine us as a nation. We know what happens when leaders succumb to the politics of fear and lose sight of our fundamental American values. Fear is what drove the government to violate the Constitution and imprison thousands of Americans of Japanese descent during World War II. Fear is what fueled the justification for torture by the CIA, which the Director objected to when he was at the Bush Justice Department. And I know the Director reminds all of his new agents that the rhetoric of fear led J. Edgar Hoover to target Martin Luther King, Jr., and others during the 1960s.

If we give in to this sort of fear, then the terrorists and extremists will have won. They want us to be afraid, and they want us to be a nation divided. Groups like ISIS, for example, actively promote the narrative that Muslims are not welcome in the United States. When there is talk about rounding up all Muslim Americans, or creating a registry based on religious beliefs, or shutting our borders to all Muslims, that is just the sort of xenophobic, hateful rhetoric that plays into our enemies' hands. It also demeans us as a democratic nation founded on the principles of freedom, equality, and liberty. We are better than that.

We are a courageous and strong country. And our strength comes from our commitment to the morals and principles that continue to keep our country great – and a beacon of democracy in the world. The Senate at its best can be the conscience of the Nation – and recent events demand that we be at our very best. We are not afraid of terrorists, and we should not let our country be defined by irresponsible fear-mongering.

While the focus of today's hearing will naturally be on the recent terrorist attacks, we should continue the Committee's bipartisan oversight of the FBI in other areas. Three years ago, the FBI learned that flawed microscopic hair comparison analysis was used in thousands of criminal prosecutions. I am not satisfied by the FBI's efforts to even notify those defendants who might be affected by the faulty evidence. The FBI should be sending agents out to gather the relevant information. The lives of potentially innocent Americans, including some on death row, depend on it. In addition, I will continue to work with Senator Grassley to ensure that whistleblowers at the FBI are afforded adequate protections.

I thank Director Comey for coming before the Committee today. I know that he shares my respect for the Constitution, and my faith in the American people to rise above the divisive rhetoric of fear.

# # # # #

Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

FOR A HEARING REGARDING

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

PRESENTED

DECEMBER 9, 2015

James B. Comey
Director
Federal Bureau of Investigation
Statement before the Senate Judiciary Committee
Washington, D.C.
December 9, 2015

Good morning Chairman Grassley, Ranking Member Leahy, 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.

Last week's tragic events in San Bernardino demonstrate these challenges. The FBI is leading a federal terrorism investigation that is on-going, wide-ranging and very complex. We continue to work closely with our federal, state and local partners as well as our foreign counterparts to review and analyze evidence to develop an understanding of the motives of the individuals involved. We are encouraging the public to channel understandable concern into an awareness and willingness to alert authorities to suspicious activities.

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

Counterterrorism remains the FBI's top priority. As we saw in Paris last month, the attack was not just an attack on Paris or the people of France – it was an attack on all of humanity and the universal values that we share. We are committed to doing everything within our power to assist our French law enforcement colleagues in bringing those responsible for this monstrous crime to justice.

The terrorist threat has changed in two significant ways. First, the core al Qaeda tumor has been reduced, but the cancer has metastasized. The progeny of al Qaeda—including AQAP, al Qaeda in the Islamic Maghreb, and the Islamic State of Iraq and the Levant (ISIL)—have become our focus. Second, we are confronting the explosion of terrorist propaganda and training on the Internet. It is no longer necessary to get a terrorist operative into the United States to recruit. Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls 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 from a decade ago.

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. These threats remain among the highest priorities for the FBI and the Intelligence Community as a whole.

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. We estimate approximately 250 Americans have traveled or attempted to travel to Syria to participate in the conflict. While this number is lower in comparison to many of our international partners, we closely analyze and assess the influence groups like ISIL have on persons located in the United States who are inspired to commit acts of violence. Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the United States and our citizens.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al Qaeda or other foreign terrorist organizations, ISIL has persistently used the Internet to communicate, and its widespread reach through the Internet and social media is most concerning. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

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 also 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.

There is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise—the inspired youth. We've seen certain children and young adults being drawn deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks.

ISIL continues to disseminate their terrorist message to all social media users—regardless of age. Following other groups, ISIL has advocated for lone offender attacks.

In recent months, ISIL released a video, via social media, reiterating the group's encouragement of lone offender attacks in Western countries, specifically calling for attacks against soldiers and law enforcement, intelligence community members, and government personnel. Several incidents in the United States and Europe over the last few months indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

The targeting of American military personnel is also evident with the release of names of individuals serving in the U.S. military by ISIL supporters. The names continue to be posted to the Internet and quickly spread through social media, demonstrating ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

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.

The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence 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 strive to work and share information more efficiently, and to pursue technological and other methods to help stay ahead of threats to the homeland.

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 is actively engaged 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 productive 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 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 intelligence analysts at the FBI Academy engaged in practical training exercises and taking core exercises together. As a result, they are better prepared to work well together in the field. Third, we've made it a priority to focus on intelligence integration training for all levels of the workforce to ensure they have the tools needed to implement, manage, and maintain successful integration of intelligence and operations. 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 the matters directly in front of us. We must also look beyond the horizon to understand the threats we face at home and abroad and how those threats may be connected. Toward that end, we gather intelligence, consistent with our authorities, to help us understand and prioritize identified threats, and to reveal the 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 priorities 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.

The FBI intelligence program's most important asset is its workforce, and we are dedicated to expanding developmental and leadership opportunities for our analysts while fulfilling the FBI's mission needs. We recently added seven senior supervisory intelligence analyst (SSIA) positions in various offices around the country to provide additional leadership opportunities for our analyst cadre and enhance our management of field intelligence work. As SSIAs, GS-15 analysts manage intelligence in the field, fulfilling a role that has traditionally been performed by an agent and demonstrating we are promoting effective integration throughout the organization.

We are also redesigning the training curriculum for another part of the intelligence program workforce—staff operations specialists (SOSs)—to aid in their performance of tactical functions in the field. In addition, a new development model clearly identifies SOS work responsibilities, tasks, training, and opportunities at the basic, intermediate, and advanced levels to guide the professional growth of SOSs across the organization at all points throughout their FBI careers.

Similarly, our language workforce continues to make important contributions to the mission. Our language professionals have recently supported numerous important investigations and operations, including Malaysia Airlines Flight 17 last summer, numerous ISIL-related investigations, the disruption of a nuclear threat in Moldova, and so many others. The National Virtual Translation Center (NVTC) also continues to provide excellent service, supporting hundreds of government offices each year. In September 2014, in recognition of the center's work providing timely, accurate, and cost-effective translation capabilities, Director of National Intelligence Clapper designated NVTC as a service of common concern to provide translation services to the Intelligence Community.

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.

This past year, the Counterintelligence and Cyber Divisions partnered to create the new Cyber-Counterintelligence Coordination Section. This new section will increase collaboration, coordination, and interaction between the divisions and will more effectively identify, pursue, and defeat hostile intelligence services using cyber means to penetrate or disrupt U.S. government entities or economic interests.

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 was 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.

Cyber

An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to strike our critical infrastructure and to harm our economy.

Between 2012 and 2014, FBI Cyber Division worked with DOJ counterparts to build a body of evidence against individuals associated with Chinese state sponsored cyber intrusion activity. This effort resulted in the criminal indictment of five officers of the People's Republic of China People's Liberation Army, Third Department (3PLA), in *United States v. Wang Dong, et al*. This action was the first indictment of uniformed state actors for malicious cyber activity. This investigation touched approximately 47 of the FBI's 56 field offices and also required novel approaches to the FBI's holdings so that prosecutors could extract the most powerful proof by integrating different sources of information. Including law enforcement efforts like these in our response will also have the intended effect of broadly changing the adversary's cost-benefit analysis when deciding to target American companies and other U.S. interests through cyber means. Accordingly, the United States government will have sent a clear message regarding international norms in cyber space—primarily that states should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors– and that it considers such activities to be criminal in nature and the subject of future and long-lasting attention by law enforcement.

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 earlier this 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, as well as other individuals for whom a federal background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

The destructive malware attack against Sony Pictures Entertainment (SPE) in late 2014 was an unprecedented cyber event for the United States in its scope, destructiveness, and economic implications. The FBI responded to this attack with an investigation that was groundbreaking in its scope and collaboration. A joint effort by the FBI investigative team, which spanned multiple field offices and Legal Attaché offices abroad,

coordinated with private partners and other government agencies to quickly establish high confidence that the Democratic People's Republic of Korea was responsible for the attack. This assessment is based upon thousands of hours of collecting forensic evidence and conducting technical analysis. The investigative team also worked to prevent additional compromises of potential victims, stop the spread of leaked SPE data, and build trust and establish a working relationship with SPE. We published unclassified threat indicators associated with the attack for use by private sector companies attempting to defend their networks from similar adversaries, and provided classified context briefings to partners in order to better protect U.S. critical infrastructure from attack. The SPE investigation highlights the degree to which effective communication between the private sector, U.S. intelligence community, and U.S. government facilitates the government's response to and investigation of cyber incidents.

Another aspect of the cyber threat that concerns us is the so-called "dark web" or "dark market." Over the past few years, the Cyber Division infiltrated Darkode, an Internet based cyber crime underground forum where cyber criminals exchanged ideas and sold tools and services enabling cyber crime. The forum's infiltration was part of Operation Shrouded Horizon, an international investigation involving twenty countries' law enforcement agencies. In August 2015, the operation culminated in a major takedown operation that resulted in global charges, arrests, and searches of 70 Darkode members and associates; U.S. indictments against 12 individuals associated with the forum, including its administrator; the serving of several search warrants in the U.S.; and the FBI's seizure of Darkode's domain name and servers. This operation executed FBI Cyber Division's strategy to target shared services of cyber crime. It was also emblematic of FBI Cyber Division's mission to identify, pursue, and defeat cyber adversaries targeting global U.S. interests through collaborative partnerships and our unique combination of national security and law enforcement authorities.

Cyber criminals frequently alter their methods and use of technology to avoid detection by law enforcement. By way of example, Cryptolocker was sophisticated ransomware that encrypted the computer files of its victims and demanded ransom for the encryption key. In May 2014, we worked with our international partners to successfully seize the domains and backend servers used to encrypt and decrypt victim machines. However, just before we did that, a new variant came into the picture.

This new ransomware, CryptoWall, is the first to use TOR— free software available to anyone online—to host the sites where victims pay their ransom. TOR—short for The Onion Router— disguises a users' identity by moving traffic between different TOR servers across the globe—one minute the traffic may be in France, the next in Russia, the next in Mexico. TOR encrypts that traffic from server to server so it is not traced back to the user. CryptoWall infections also pay ransom with Bitcoin, rather than with traditional currency.

All this gives cyber criminals an additional layer of anonymity that makes them even more difficult to track, and it shows how easily our adversaries can step up their game to avoid detection by law enforcement. Our estimates are that there are more than 800,000 victims worldwide, with demands for ransom ranging anywhere from $200 to

$5,000. We're working with our partners overseas to bring down CryptoWall, just like we brought down its predecessor.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques—such as sources, court-authorized electronic surveillance, physical surveillance, and forensics—to fight the full range of cyber threats. We are working side-by-side with our federal, state, local, and tribal partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF), which serves as a coordination, integration, and information sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations.

Through CyWatch, our 24-hour cyber command center, 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.

Weapons of Mass Destruction

The FBI, along with its U.S. government partners, is committed to countering the threat of nuclear smuggling and ensuring that terrorist groups who may seek to acquire these materials are never able to do so. The FBI and Moldovan authorities have worked closely to combat this threat for a number of years. These efforts included investigative and technical assistance, as well as capacity-building programs with our U.S. government partners, to enhance the Republic of Moldova's ability to detect, investigate, and prosecute nuclear and radiological smuggling.

In the spring of 2014, the FBI supported two joint investigations targeting WMD trafficking in Moldova. These operations targeted two separate networks that were smuggling allegedly radioactive material into Moldova; the operations resulted in arrests by Moldovan Police in December 2014 and February 2015. Depleted and natural uranium were seized in December 2014, and an unknown, liquid metal contained in an ampoule, purported to be cesium, was seized in February 2015.

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

Crimes of hatred and prejudice—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 and beyond. When a teenager is murdered because he is gay, we all feel 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. According to our most recent statistics, hate crime has decreased slightly in neighborhoods across the country, but the national numbers remain sobering.

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

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 over 2,700 pending health care fraud investigations. Over 70 percent of these investigations involve all government funded programs to include Medicare, Medicaid, CHIP, VA, DoD, and 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 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, local, and tribal officers and deputies on joint task forces and individual investigations.

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

In support of the Department of Justice, Bureau of Justice Assistance's Violence Reduction Network, the FBI developed a comprehensive 10-point crime reduction strategy in order to "unlock" all of the technical and investigatory resources of the FBI in assisting local and state agencies. The strategy highlights key technological and investigative capabilities which the FBI can deploy to assist local agencies. These services include the following: use of the FBI forensic, technology, and computer laboratories; use and deployment of the Cellular Analysis Survey Team and tracking teams; use of Video Recovery Teams and training in digital imaging; source development and payments; media strategies and billboard displays; intelligence training and analytical assistance; victim witness coordination and community impact; homicide reduction initiative/Save our Streets Initiative; National Center for the Analysis of Violent Crime and the Behavioral Analysis Unit; and the Violent Criminal Apprehension Program (ViCap).

These services have been effectively utilized by the initial five Violence Reduction Network (VRN) cities, Camden, New Jersey; Wilmington, Delaware; Chicago, Illinois; Oakland/Richmond, California; and Detroit, Michigan. During fiscal year 2016, five additional cities are being incorporated within the VRN, specifically Compton, California; Little Rock, Arkansas; West Memphis, Arkansas; Newark, New Jersey; and Flint, Michigan.

Despite these efforts, there is something deeply disturbing happening all across America. The latest Uniform Crime Reporting statistics, *Crime in the United States, 2014*, show that the number of violent crimes in the nation decreased, but this year we are 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. We simply do not know for sure.

Need for Incident-Based Crime Data

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

Furthermore, demographic data regarding officer-involved shootings is not consistently reported to us through our Uniform Crime Reporting program. We in the FBI track and publish the number of "justifiable homicides" by police officers. But such reporting by police departments across the country is not mandatory, and perhaps lacks sufficient

incentive, so not all departments participate. The result is that currently we cannot fully track incidents involving use of force by police. And while the *Law Enforcement Officers Killed and Assaulted* report tracks the number of officers killed in the line of duty, we do not have a firm grasp on the numbers of officers assaulted in the line of duty. We cannot address concerns about officer-involved shootings if we do not know the circumstances surrounding such incidents.

We need to improve the way we collect and analyze data so that we see the full scope of what is happening in our communities. One way to do this is to increase participation in the National Incident-Based Reporting System (NIBRS). NIBRS includes more than mere summary statistics—the numbers of robberies or homicides across the country each year. It gives the context of each incident, giving us a more complete picture. We can use it to identify patterns and trends, and to prevent crime.

We also need a system to capture the use of force statistics on all non-fatal/fatal police officer-involved incidents. We can use this information to tell us where we may have problems, and what we need to do to improve the way we police our communities.

Unfortunately, only a little more than one third of our state, local, and tribal partners submit data to NIBRS. One of the fears of police chiefs and sheriffs across the country is that by submitting data to NIBRS, they may see an increase in statistics on criminal activity. However, an increase in statistics is not the same thing as an actual increase in crime. It means we are more accurately reporting what is happening in our communities. We hope to resolve that issue by phasing in NIBRS over the next few years, and overlapping it with the summary reporting system.

Police chiefs and sheriffs also worry about the cost of implementing a new reporting system with new software, during a time when budgets are already tight. We are working with the Department of Justice to find funding, because NIBRS is important. It is a matter of short- term pain for long-term gain.

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

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. .

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. One such undercover investigation led to the conviction earlier this year of an Alaskan man who produced child pornography in Cambodia and brought it to the United States, and who helped others plan to abuse children abroad.

These strategies include a multi-disciplinary approach through partnerships with foreign law enforcement and non-governmental organizations to provide child victims with available support services. Similarly, the FBI's Innocence Lost National Initiative serves as the model for the partnership between federal, state, local, and international law enforcement partners in addressing child prostitution. Since its inception, more than 4,350 children have been located and recovered. The investigations and subsequent 1,950 convictions have resulted in lengthy sentences, including 15 life terms.

Indian Country

There are 566 federally recognized Indian 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 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.

Active Shooter Training

In response to the Sandy Hook school shooting, the president took steps to protect children and communities by reducing gun violence. He assigned the vice president to lead the effort with a focus 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 11,000 senior state, local, tribal, and campus law enforcement executives at conferences hosted by FBI field offices, and we have trained more than 7,000 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 31,500 officers from 5,600 agencies.

We have made a good start training our state, local, and tribal partners on how to handle these incidents, and we have built stronger partnerships along the way. In an effort to spread best practices and lessons learned more broadly, we produced a 40-minute film, *The Coming Storm*, that was distributed to more than 10,000 of our partners at the International Association of Chiefs of Police conference in October. The

film ultimately has the potential to reach more than three million law enforcement and emergency response personnel. Featuring first-person accounts from police chiefs, first responders, and victims involved in country's most tragic shooting scenes—including Virginia Tech, Sandy Hook, and Aurora—*The Coming Storm* aims to train viewers how best to respond to and recover from a large-scale incident.

Five Eyes Law Enforcement Group

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

FBI Laboratory

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

The Terrorist Explosives Device Analytical Center (TEDAC) is another example. TEDAC was formally established in 2004 to serve as the single interagency organization to receive, fully analyze, and exploit all priority terrorist improvised explosive devices (IEDs). TEDAC coordinates the efforts of the entire government, including law enforcement, intelligence, and military entities, to gather and share intelligence about IEDs. These efforts help disarm and disrupt IEDs, link them to their makers, and prevent future attacks. Although originally focused on devices from Iraq and Afghanistan, TEDAC now receives and analyzes devices from all over the world.

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

Additionally, the Laboratory Division maintains a capability to provide forensic support for significant shooting investigations. The Laboratory Shooting Reconstruction Team provides support to FBI field offices by bringing together expertise from various Laboratory components to provide enhanced technical support to document complex shooting crime scenes. Services are scene and situation dependent and may include mapping of the shooting scene in two or three dimensions, scene documentation through photography, including aerial and oblique imagery, 360 degree photography and videography, trajectory reconstruction, and the analysis of gunshot residue and shot patterns. Significant investigations supported by this team include the shootings 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.

The FBI is actively participating in and helping to lead the Intelligence Community Information Technology Enterprise (IC ITE), an Office of the Director of National Intelligence-led, multi-year initiative to move the Intelligence Community from agency-centric IT systems and architectures to a common IT environment to promote intelligence integration, collaboration, and efficiency. The primary objective is to enhance mission effectiveness through better technology integration. The IC ITE provides value to the FBI by enabling our agents and analysts to share and leverage data, information, applications, and tools with the Intelligence Community in a common environment which facilitates real-time communication and collaboration. In addition, the FBI is developing efficient and effective processes for migrating certain data sets and applications to the Intelligence Community cloud in accordance with Department of Justice and Intelligence Community statutes and policies.

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.

By way of example, the FBI recently entered into a contract to deliver a virtual desktop solution to 55,000 FBI employees, private contractors, and other government employees working with the FBI on one of the largest virtual desktop infrastructure deployments in the government. The virtual desktop will allow employees to access multiple enclaves of varying classification levels from one workstation while ensuring that all data is protected and segregated according to classification. It will also lower the FBI's total cost of ownership while expanding information availability to more employees.

The FBI is enhancing personnel safety, efficiency, and effectiveness with "just-in-time" delivery of information and services to our mobile workforce. The FBI recently deployed more than 30,000 smartphones to employees in all 56 field offices over a four-month period, addressing what was seen as a major capability gap. Using the device as the basic portable platform, the FBI has been able to deploy additional field capabilities, ranging from fingerprint collection and analysis in the field to improved situational awareness between various tactical teams and surveillance operations.

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

Chairman Grassley, Ranking Member Leahy, 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.