OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

OCTOBER 22, 2015

Serial No. 114–55

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

97–262 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
MIMI WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MIKE BISHOP, Michigan

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

CONTENTS

OCTOBER 22, 2015

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

THURSDAY, OCTOBER 22, 2015

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to call, at 10:15 a.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Smith, Chabot, Issa, Forbes, King, Franks, Gohmert, Poe, Chaffetz, Marino, Labrador, Collins, DeSantis, Buck, Ratcliffe, Trott, Bishop, Conyers, Lofgren, Jackson Lee, Cohen, Johnson, Chu, Deutch, Gutierrez, Bass, DelBene, Jeffries, Cicilline, Peters.

Staff Present: (Majority) Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Chief of Staff & Chief Counsel; Allison Halataei, Parliamentarian & General Counsel; Jason Herring, FBI Detailee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Caroline Lynch, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Robert Parmiter, Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Ryan Breitenbach, Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Kelsey Williams, Clerk; (Minority) Perry Apelbaum, Staff Director & Chief Counsel; Aaron Hiller, Chief Oversight Counsel; Joe Graupensperger, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Tiffany Joslyn, Deputy Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Eric Williams, Detailee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; and Veronica Eligan, Professional Staff Member.

Mr. GOODLATTE. Good morning. The Judiciary Committee will come to order. And without objection, the Chair is authorized to declare recesses of the Committee at any time.

We welcome everyone to this morning's hearing on the oversight of the Federal Bureau of Investigation, and I will begin by recognizing myself for an opening statement.

Welcome, Director Comey, to your second appearance before the House Judiciary Committee since your confirmation as the seventh Director of the Federal Bureau of Investigation. We are happy to have you here with us today. I once again commend your distin-

guished service to our Nation, and I'm confident you will continue to serve honorably at the helm of the FBI.

Today, the FBI continues to face the effects of one of the worst national security leaks in our Nation's history by Edward Snowden 2 years ago. Over the past year, the House Judiciary Committee spearheaded the passage of the USA FREEDOM Act, a bipartisan law that ended a controversial national security program and provided expanded oversight and transparency of America's intelligence gathering. The USA FREEDOM Act ensures that Federal law appropriately respects civil liberties while providing the necessary tools to preserve our collection capabilities and thereby meet our national security responsibilities.

I want to again thank Director Comey and the men and women of the FBI for working closely with Members of this Committee to ensure passage and enactment of the USA FREEDOM Act.

Events over the past year in the Middle East have deeply violated the world's moral compass with scenes of unimaginable brutality at the hands of ISIS. In particular, the appalling and indiscriminate targeting of anyone who fails to abide by ISIS' stated goal to establish a global caliphate has resulted in the shedding of innocent blood by the most revolting methods.

As a radical Islamic terrorist organization, ISIS mandates conformity to an ideology which permits no dissent. As Americans with a strong history of protecting religious liberty, we stand in total opposition to ISIS' decimation of Christian populations in the Middle East and to its vicious tactics.

America is not immune to ISIS' propaganda of terror. American teenagers have been radicalized in part by ISIS' concerted social media efforts promoting the killing of fellow Americans, and just last week a like-minded cyber hacker was indicted for providing ISIS with information on U.S. service members.

Director Comey, you are at the forefront of protecting our country from those who patiently plot to do us harm, and I am interested today in hearing more about the FBI's efforts to combat ISIS.

Over 3 years ago, our diplomatic mission to Benghazi, Libya, was attacked by terrorists and four Americans, including our Ambassador, were killed. As of today, only one subject has been apprehended and placed on trial. I am interested in hearing more from you about the status of the FBI's investigation and efforts to bring to justice other terrorist killers who murdered four of our citizens.

Separately, it was revealed this past year that former Secretary of State Hillary Clinton used a private e-mail server to conduct her official business while serving as Secretary of State. Two inspectors general have already reported that classified information was contained within Secretary Clinton's private e-mail and have referred the matter to the Justice Department.

While the apparent lack of transparency related to the use of a private server to conduct the Nation's diplomatic business is troubling, it also raises significant questions concerning the security of national secrets and the potential insight that such a home-brew setup may afford a foreign intelligence service into the day-to-day digital record of a top-level government official.

On the technology front, the issue known as Going Dark has been at the top of the FBI's concerns in recent years. Encryption

technology is exciting and can effectively secure private communications when privacy is needed or desired. In fact, over 15 years ago, I led congressional efforts to ensure strong encryption technology and to ensure that the government could not automatically demand a backdoor key to encryption technologies.

This enabled the U.S. encryption market to thrive and produce legitimate encryption technologies for legitimate actors rather than see the market head completely overseas to companies that do not have to comply with basic protections. However, it is true that this technology can also be used by those who wish to do us harm. Adoption of new communications technologies by those intending to harm the American people is outpacing law enforcement's technological capability to access those communications in legitimate criminal and terrorist investigations.

In light of the Administration's recent announcement that it is not currently seeking a legislative solution to its Going Dark challenges, I am interested to hear your perspective on whether the Administration's newly announced approach to work in an ad hoc fashion with communication providers is an adequate solution.

Finally, violent crime appears to be on the rise across the country, particularly around our major metropolitan centers. It is disconcerting to watch the gains of the past decades unravel in an explosion of community violence. We have also witnessed several incidents in the past year that, unfortunately, have led to increased community tension with law enforcement. This tension will hopefully be resolved through improved communication, accountability, policing practices, and various other initiatives.

I hope to hear the FBI's perspectives on the reasons for the increase in crime and how to ensure that law enforcement officers and the citizens they serve can coexist in a safe and respectful environment.

In conclusion, Mr. Director, please know that this Committee sincerely appreciates your efforts to keep us safe and the heroic actions consistently performed by the men and women of the FBI to protect our country. I look forward to hearing your answers on all of these important topics today, as well as on our other issues of significance to the FBI and our Nation.

At this time, I am pleased to recognize the Ranking Member of the Committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

Mr. CONYERS. Thank you, Chairman Goodlatte.

Good morning, Director Comey. We welcome you for this second appearance before the House Judiciary Committee since taking office on September the 4th, 2013.

The FBI's mission is a complex undertaking to protect the United States from terrorism, to enforce our criminal laws, and to lead the Nation's law enforcement community. And yet, as vast as this mission seems, I think nearly all of the discussion we will have here today can be distilled into one word: Trust. Trust in the executive branch to respect and secure our privacy and our civil liberties. Trust in the FBI as an institution. Trust in State and local agencies that police our communities.

In many respects, Director Comey, I think we agree on this point. For example, you have spoken powerfully about the hard

truths we must keep in mind when we discuss race and policing, and particularly when we discuss the use of force by police officers. I am told that you require all new agencies to study the FBI's interaction with Dr. Martin Luther King, Jr., and to visit his memorial at the Tidal Basin. I'm also advised that you keep on your desk a copy of Robert Kennedy's approval of J. Edgar Hoover's request to place a wiretap on Dr. King.

These are powerful reminders of a troubling and not-too-distant history. It's not difficult to draw a line from that era to recent events in Ferguson, Baltimore, New York, and Cleveland. And that's why your work to build trust between police and our communities is so important.

Nowhere is that effort more apparent than in your call for better data on the use of force by police. Although the FBI is the national custodian of crime statistics, that data is reported voluntarily and inconsistently. You have been honest in your assessment that official statistics in this area are so incomplete as to be embarrassing and ridiculous.

We need a better understanding of what drives police use of force, and we cannot study the problem without reliable data. I urge you to continue to press your State and local partners for consistent and accurate reporting to the National Incident-Based Reporting System.

Just as we must rebuild trust in certain State and local law enforcement units, we will look to your testimony today to reassure us about a number of programs and activities at the FBI. Earlier this year, the public noticed a small plane flying in a tight pattern directly over the site of unrest in west Baltimore. Other reports from other parts of the country, including my own district in Detroit, raise questions about the presence of similar aircraft.

The FBI has since confirmed the existence of its aerial surveillance program. On June 3, 15 Members of this Committee wrote you to ask for more information about this program. Your team provided our staff with a briefing soon thereafter. But the public still has many questions about aerial surveillance, and you have said that there is a great deal of misinformation about this program. I would like you to use your testimony and presence here today to explain from your perspective how this program works and why we should trust the Bureau to operate it.

Similarly, I think we would benefit from a fuller description of encryption and what you've called the Going Dark problem. Over the past year, you have called for a congressional mandate to give the FBI special access to otherwise encrypted data.

I have a difficult time understanding this proposal. Every technical expert who has spoken on this issue has concluded that it is technically impossible to provide this access without also compromising our security against bad actors. Even if it were technically feasible, it would cost our technology sector perhaps billions of dollars to implement the scheme and perhaps billions more from loss of business overseas where the United States Government surveillance programs have already taken a toll on the industry.

And even if it were technically feasible and easy to implement, a new rule for United States companies would not succeed in keep-

ing bad actors from using unbreakable encryption, which is open source, free, and widely available from companies based overseas.

As Chairman Goodlatte argued when we had this debate in 1999, only by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment. I agree with that sentiment, and you have made similar public statements, and I hope that you can help us to reconcile that view with your call for special access.

And finally, because rigorous oversight is necessary for public trust, I hope that you will commit today to full compliance with the Inspector General Act. For the past 5 years, the FBI has resisted the clear mandate of that law. The inspector general of the Department of Justice is to have timely access to every document he requires to carry out his duties.

Noncompliance has real consequences. This Committee waited until February of this year to receive a report about the FBI's use of Section 215 orders from 2007 to 2009. The public waited until May for the unclassified version. In the middle of a national debate on government surveillance, we waited 6 years for critical information. This delay is unacceptable.

I understand that there are other interpretations of the law. Congress will soon clarify the matter, likely in overwhelmingly bipartisan fashion. But in the meantime, Director Comey, I hope that the Bureau will step away from its litigating position and give the Office of the Inspector General the access it requires and deserves.

Your job is a complex and demanding one, Director. We appreciate you being here today, and I look forward to your testimony.

And I thank the Chairman and yield back.

Mr. GOODLATTE. Thank you, Mr. Conyers.

Without objection, all other Members' opening statements will be made a part of the record.

We welcome our distinguished witness today. And if you'll please rise, we'll begin by swearing you in.

Do you swear that the testimony that you are about to give shall be the truth, the whole truth and nothing but the truth, so help you God?

Director COMEY. I do.

Mr. GOODLATTE. Thank you.

Let the record reflect that the witness has responded in the affirmative.

On September 4, 2013, Director Comey was sworn in as the seventh director of the FBI. He began his career as an assistant United States attorney for both the Southern District of New York and the Eastern District of Virginia. After the 9/11 terrorist attacks, Director Comey returned to New York to become the United States attorney for the Southern District of New York. In 2003, he was appointed Deputy Attorney General under United States Attorney General John Ashcroft. Director Comey is a graduate of the College of William and Mary and the University of Chicago Law School.

We welcome you again today to your second appearance before the House Committee. Your written statement will be entered into the record in its entirety, and we ask that you summarize your tes-

timony in 5 minutes. And with that, we welcome you again to the Committee.

TESTIMONY OF THE HONORABLE JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. COMEY. Thank you, Chairman Goodlatte, Congressman Conyers. It's good to be back before you and the Members of the Committee for my second annual oversight hearing. I expect to be back for eight more during my 10-year term, which I look forward to very much.

What I thought I would do is just explain to the Committee in very short form how we at the FBI think about ourselves and a couple of the things that are prominent in our work today. I think the FBI can best be described in a single sentence: We are a national security and law enforcement organization that uses, collects, and shares intelligence in everything that we do.

That sentence captures us in two different ways. First, the first half of that sentence, we are a national security and law enforcement organization. There is great strength to the American people in having our criminal responsibilities and our national security responsibilities in the same place.

Perhaps no better example is there of the strength that's gained from that combination than the rule of law as the spine of the FBI. It is a great thing, I think, for this country that the people responsible for counterintelligence, counterterrorism, and the criminal work all have as part of their being the rule of law and the Bill of Rights.

The second half of that sentence, we use, collect, and share intelligence in everything that we do, is a description of what I think we have always been but what we have tried to get so much better at since 9/11. That is being thoughtful about what we know, what we need to know, and who needs to know what we know so that we can all be more effective in protecting this country.

I want to touch on two topics under our responsibilities. Start with national security. The threat posed to us from ISIL's crowdsourcing of terrorism using social media is a significant feature of our work. It was an especially taxing threat the FBI dealt with earlier this summer when all over the country, in hundreds of investigations, we were trying to evaluate where people are from consuming ISIL's poison to acting on it.

Through the Internet, the so-called Islamic State has been pushing a twin-pronged message to troubled souls all over the world and all over our country. The first prong is come to the so-called caliphate and live a life of glory; and if you can't come, the second prong says, kill. Kill where you are. Kill anyone. If you can kill people in uniform, military or law enforcement, best of all.

That message has gone out since the summer of 2014 aggressively and in a very sophisticated way to thousands of consumers on Twitter. And Twitter works to sell books or movies or magazines. It works to crowdsource terrorism. And so in every State we have investigations trying to understand where people are on the path from consuming to acting.

And this is a very different paradigm than the traditional Al Qaeda paradigm because this is not about national landmarks and

sophisticated, long-tail, carefully surveilled events. This is about trying to motivate murder anywhere, by anyone. And, unfortunately, it's a message that resonates with troubled souls seeking meaning.

And so earlier this summer, especially in May, June, and July, we were faced with the prospect of a whole lot of people acting out on this inspiration or direction from ISIL, and thanks to great work by the men and women of the FBI and our partners in State, local, and Federal law enforcement, we disrupted a whole lot of efforts to murder innocent people in the United States.

That work, though, continues, and it is made particularly difficult by an issue both you and Mr. Conyers touched upon. Our mission is to find needles in a nationwide haystack, and we have hundreds of investigations aimed at doing that in all 50 States. But increasingly what ISIL does is move the real live ones who might be willing to kill on their behalf off of Twitter to a mobile messaging app that is end-to-end encrypted. And at that moment, the needle that we may have found becomes invisible to us even with court orders, which is how the FBI does its business.

And so that's the challenge we face called Going Dark in real living color. We are trying to interdict, trying to stop, trying to understand people on the cusp of acts of violence, and increasingly a tool that the American people count on us to use is less and less effective. I don't know exactly what to do about that, frankly, but I think my job, given the responsibility I have, is to tell people there's a problem and we need to talk about it. And so I look forward to a conversation about it with you.

Our law enforcement responsibilities is the second thing I just want to touch very briefly. Obviously, we do public corruption work. We protect children. We fight fraud. We do a whole lot of work with our partners around the country to address violent crime. Something very disturbing is happening in this country right now in law enforcement and in violent crime.

I imagine two lines, one being us in law enforcement and the other being communities we serve and protect, especially communities of color. Those two lines over the last year or so have been arcing away from each other, and that continues. Each incident that involves police misconduct or perceived misconduct bends one line away. Each time an officer is killed or attacked in the line of duty bends the other line farther away.

And in the midst of those arcing away from each other, maybe because they're arcing away from each other, we are seeing a dramatic spike in violent crime, especially homicide, in cities all across the country. In communities of color especially, especially young men are dying at a rate that dwarfs what we've seen in recent history. It's happening all over the country, and it's happening all in the last 10 months.

And so a lot of us in law enforcement are talking and trying to understand what is happening in this country, what explains the map we see, what explains the calendar. Why is it happening all over the country? Why is it happening this year?

I don't know the answer to that. I, as I said, like a lot of people in law enforcement, are struggling with it. We simply must focus on this because all lives matter. This is not a problem America

should drive around. We should stare at it. And as we stare at it, we should all work for ways to bend those lines back toward each other, because we need each other. We need each other to make sure our communities are safe. We have achieved in 2014 historically low violent crime in this country. We cannot let that slip away from us.

I am grateful for the hard work of the men and women of the FBI on these challenges. I am especially grateful for our partners in law enforcement around the country who help us address those. As you know, the FBI doesn't have a lot of fancy stuff. We have people, and we have great people, thank goodness, who are Americans who care deeply about protecting all their fellow citizens. I am honored to be in this job where I get to watch what they do and help them. And I look forward to your questions.

[The prepared statement of Mr. Comey follows:]

Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED
OCTOBER 22, 2015

Statement of
James B. Comey
Director
Federal Bureau of Investigation

Before the
House Committee on the Judiciary
United States House of Representatives

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

October 22, 2015

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

Today's FBI is a threat-focused, intelligence-driven organization. Each FBI employee understands that to defeat the key threats facing our nation, we must constantly strive to be more efficient and more effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and our communities. These diverse threats underscore the complexity and breadth of the FBI's mission.

We remain focused on defending the United States against terrorism, foreign intelligence, and cyber threats; upholding and enforcing the criminal laws of the United States; protecting privacy, civil rights and civil liberties; and providing leadership and criminal justice services to Federal, State, 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; however, the 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 drawing 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, and local 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. As a result, the FBI and all law enforcement organizations must understand the latest communication tools and position ourselves to identify and prevent terror attacks in the homeland.

We live in a technologically driven society, and just as private industry has adapted to modern forms of communication, so too have terrorists and criminals. Unfortunately, changing forms of Internet communication and the use of encryption are posing real challenges to the FBI's ability to fulfill its public safety and national security missions. 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.

Encryption impacts nearly all of our cyber operations now that our adversaries are becoming better and better at what they do. 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 – a free software available to anyone online – to host the sites where victims pay their ransom. The TOR Network – 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.

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 and local 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. Towards 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, research and development, intellectual property, and insider information from the Federal government, U.S. corporations, and American universities. Foreign intelligence entities continue to grow more

creative and more sophisticated in their methods to steal innovative technology, critical research and development data, and intellectual property. Their efforts seek to erode America's leading edge in business, and pose a significant threat to our national security.

We remain focused on the growing scope of the insider threat – that is, when trusted employees and contractors use their legitimate access to information to steal secrets for the benefit of another company or country. This threat has been exacerbated in recent years as businesses have become more global and increasingly exposed to foreign intelligence organizations.

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 Entities List investigations. The HTC is the first of its kind in the FBI; it has been well-received in the US 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 US 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 at 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 seventy Darkode members and associates; U.S. indictments against twelve 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.

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, and local 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 US 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 US 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 and local authorities in pursuing these cases.

One key focus is border corruption. The Federal government protects 7,000 miles of U.S. land border and 95,000 miles of shoreline. Every day, more than a million visitors enter the country through one of 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.

Healthcare Fraud

We have witnessed an increase in healthcare 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 Healthcare Fraud investigations. Over 70% 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 and local 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 Healthcare Fraud Prevention Partnership, an effort to exchange facts and information between the public and private sectors in order to reduce the prevalence of Healthcare 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 and local officers and deputies on joint task forces and individual investigations.

FBI joint task forces – Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces – focus on identifying and targeting major groups operating as criminal enterprises. Much of the Bureau's criminal intelligence is derived from our State, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

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, NJ; Wilmington, DE; Chicago, IL; Oakland, CA; and Detroit, MI. During FY16, five additional cities are being incorporated within the VRN, specifically Compton, CA; Little Rock, AR; West Memphis, AR; Newark, NJ; and Flint, MI.

Despite these efforts, there is something deeply disturbing happening all across America. Although 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. Those police chiefs report that the increase is almost entirely among young men of color, at crime scenes in bad 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, from the return of violent offenders to their communities following jail terms and the availability of synthetics and inexpensive heroin to the accessibility of guns or a change in policing in the so-called YouTube era. 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 law enforcement "use of force" policies and 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 and local 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, and international partners. The Bureau continues to share intelligence about criminal groups with our partners and 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 149 child victims of all races and arresting 153 pimps and 106 Johns. Ninety Victim Specialists, in coordination with local law enforcement victim advocates and non-governmental organizations, provided nearly 2,200 services to 105 child victims and 490 adult

victims. From the first Operation Cross Country to this most recent action, 755 children have been recovered and 1,015 pimps have been arrested.

The FBI established the Child Sex Tourism Initiative to employ proactive strategies to identify U.S. citizens who travel overseas to engage in illicit sexual conduct with children. These strategies include a multi-disciplinary approach through partnerships with foreign law enforcement and non-governmental organizations to provide child victims with available support services. 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 567 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 and local 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 will be distributed to more than 10,000 of our partners at the International Association of Chiefs of Police conference next week. 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 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 (FBI), Drug Enforcement Administration (DEA), U.S. Immigration and Customs Enforcement, Homeland Security Investigations (HSI), the UK's National Crime Agency (NCA), the Royal Canadian Mounted Police (RCMP), the Australian Federal Police (AFP), Australian Crime Commission (ACC), and New Zealand Police (NZP). 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 blends forensic science and computer technology into a highly effective tool for linking crimes. It enables Federal, State, and local forensic labs to exchange and compare DNA profiles electronically, thereby connecting violent crimes and known offenders. Using the National DNA Index System of CODIS, the National Missing Persons DNA Database helps identify missing and unidentified individuals.

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

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 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 (IC).

The FBI is actively participating 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 IC 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 IC 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 IC Cloud in accordance with Department of Justice and IC 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 IC partners around the world.

Conclusion

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

I look forward to answering any questions you may have.

###

Mr. GOODLATTE. Thank you, Director Comey.

We'll now proceed under the 5-minute rule with questions for the Director, and I'll begin my recognizing myself.

Since the passage of the USA FREEDOM Act, a law that struck a balance between privacy and national security, is the FBI experiencing any difficulty in complying with the new law?

Mr. COMEY. We have not, Mr. Chairman. We haven't yet gotten to the place where the alternative system for telephone metadata has been built, but so far we haven't seen an adverse impact.

Mr. GOODLATTE. But you're getting very close to that, I think——

Mr. COMEY. Yes, sir.

Mr. GOODLATTE [continuing]. The date when the metadata collection will be completely turned off?

Mr. COMEY. Yes. The end of next month, I believe.

Mr. GOODLATTE. Even with a decade's worth of information on Iraqi refugees, didn't we still encounter cases of domestic terrorism conducted by those admitted as refugees? With significantly less information on potential Syrian refugees, isn't it true that you can't ensure that the Iraqi experience is not going to be replayed?

Mr. COMEY. Thank you, Mr. Chairman.

Yes, you're correct that we did discover in people who had come in as refugees from Iraq a number of people who were of serious concern, including two that were charged when we found their fingerprints on improvised explosive devices from Iraq. And there's no doubt that that was the product of a less-than-excellent vetting that had been done on Iraqi refugees.

There's good news and bad news. The good news is we have improved dramatically our ability as an interagency, all parts of the U.S. Government, to query and check people. The bad news is our ability to touch data with respect to people who may come from Syria may be limited. That is, if we don't know much about somebody, there won't be anything in our database.

Mr. GOODLATTE. In fact, much less than we had access to when we were in Iraq——

Mr. COMEY. I think that's fair.

Mr. GOODLATTE [continuing]. And had extensive networking and access to information about Iraqi citizens that simply does not in any way compare to the lack of information we have today about Syrian nationals who are seeking refugee status in the United States.

Mr. COMEY. I think that's a fair generality, that the data we had available to us from Iraq from a decade of our folks being there, encountering people, is richer than the data we have from Syria.

Mr. GOODLATTE. The Director of the National Security Agency has said that former Secretary of State Clinton's private e-mail server would be a sought-after target for a foreign intelligence agency. Do you also believe that a foreign intelligence agency, particularly an adversary's, could benefit from acquiring and exploiting sensitive and classified information of a top-level U.S. Government official?

Mr. COMEY. Mr. Chairman, I'd respectfully say that's one I'm not going to comment on. As you know, the FBI is working on a referral given to us by inspectors general in connection with former Secretary Clinton's use of a private e-mail server. As you also know

about the FBI, we don't talk about our investigations while we're doing them. This is one I'm following very closely and get briefed on regularly. I'm confident we have the people and the resources to do it in the way I believe we do all our work, which is promptly, professionally, and independently. But I don't want to do anything that would compromise my ability to do it that way by commenting beyond that.

Mr. GOODLATTE. Well, how about answering my generic question, not directed at the specifics of that case, but rather the question of whether you believe that a foreign intelligence agency, particularly an adversary's, could benefit from acquiring and exploiting sensitive and classified information of a top-level U.S. Government official?

Mr. COMEY. Thank you, Mr. Chairman. I hope you'll understand why I don't think it's appropriate for me to answer that. I want to preserve my ability to oversee this investigation in a way that is both in reality independent and fair and is perceived that way.

I believe the Bureau is three things. We are competent, we're independent, and we're honest, and I want to make sure the American people have confidence that that's the way we're doing our business. And if I start answering questions like yours, which is a reasonable question, I worry that I could infringe upon that.

Mr. GOODLATTE. You've said that encryption represents the Going Dark problem in high definition. Earlier this month you testified in front of the Senate Homeland Security and Governmental Affairs Committee that the Obama administration has decided to no longer seek a legislative remedy to address challenges law enforcement faces with encryption and Going Dark. What has changed? And do you agree with the concerns that I and the Ranking Member, Mr. Conyers, have expressed about some of the proposals that had previously been made with regard to addressing this problem?

Mr. COMEY. I think what the Administration has decided, Mr. Chairman, is that it is not going to seek a legislative remedy now so that we can continue the conversations we're having with the private sector, with our allies around the world, and with State and local law enforcement, who are hugely impacted by this, and I think that makes good sense. I don't think we are yet to a place where we know exactly so how would we fix this legislatively. This is a very hard problem.

I think you and Mr. Conyers have raised serious questions and concerns. I believe this is an incredibly hard problem because two sets of values we all care about, safety and security on the Internet. I'm a big fan of strong encryption for the reasons you said. It helps us fight cybersecurity. It helps us protect all that matters most to us personally and as a Nation and public safety that we all care about. And those two things are colliding with each other.

There's not an easy answer, but given how important both of those values are and what's at stake, I think we have to wrestle with it, and we are continuing to do that. We're having very good conversations along all the dimensions I just said, and we'll continue it, I hope.

Mr. GOODLATTE. I just came from a meeting with Bill Gates who indicated that the progress being made in quantum computing is

dramatic and that computers of that high capability will soon be able to crack any kind of encryption that anyone has. That I found to be very interesting information. I have both good and bad views of that because obviously that can be seriously abused and invade the privacy of law-abiding citizens, but it also will be a source of solving your problem when you encounter encrypted materials by people who are suspected enemies of the United States or criminals capable of using high technology to protect themselves and evade prosecution under the law.

Do you have any comments or knowledge about the current state of quantum computing?

Mr. COMEY. Nothing that would be useful to you. I've read about it in the popular press. I only have 8 years left in my term. I have a hard time imagining a police officer in New York City in a kidnapping case having access to a quantum computer any time in the near future when they encounter a device that's locked. And so it may be some day that's an answer to the challenge, to the conflict of those two sets of values. I don't see it anywhere near in the near term.

Mr. GOODLATTE. Thank you.

I now recognize the Ranking Member for his questions.

Mr. CONYERS. Thank you, Mr. Chairman.

Welcome again, Director Comey.

You observed that The Washington Post and The Guardian are becoming the lead source of information about violent encounters between police and civilians. You called the state of FBI statistics on these accounts embarrassing and ridiculous. And now that you've had some time to reflect on them, do you stand by this comment?

Mr. COMEY. I do, Mr. Conyers. I think it's embarrassing for those of us in government who care deeply about these issues, especially the use of force by law enforcement, that we can't have an informed discussion because we don't have data. People have data about who went to a movie last weekend or how many books were sold or how many cases of the flu walked into an emergency room, and I cannot tell you how many people were shot by police in the United States last month, last year, or anything about the demographics, and that's a very bad place to be.

Mr. CONYERS. Why, sir, does the FBI have trouble collecting this information?

Mr. COMEY. I think the big challenge, Mr. Conyers, is that it requires cooperation from 18,000 law enforcement organizations all around the country, and we are a big, diverse country of many different size organizations in the law enforcement space, and so we have never all sat together and said let's change the way we do this, and I'm optimistic we're about to do that.

Mr. CONYERS. You're working on the problem——

Mr. COMEY. Very hard.

Mr. CONYERS [continuing]. And you think that it's coming together.

Mr. COMEY. Very hard. And the good news is chiefs and sheriffs get it and want to be in a position we as a country can have informed conversations. And so what I have been asking for resonates with them. I'm going to speak to them again at a huge con-

ference in Chicago next week. And I'm optimistic that we can get to a much better place. It's going to take us a few years, but I think we can get to a much better place.

Mr. CONYERS. I hope so. Your written testimony takes a rather dim view of the so-called Going Dark problem. You want private companies to understand the public safety and national security risks that result from malicious factors' use of their encrypted products and services. In the past you have balanced comments like these with an honest assessment of the benefits of strong encryption. I want you to take some time to do that here. Why is encryption important to the Internet economy, to cybersecurity, and in many cases to our personal security?

Mr. COMEY. Encryption is vital to our personal security because all of our lives are now online. I like people locking their cars when they go into a store. I like people to lock their homes so that people can't break in and steal what matters to them. Now what matters to us as people and as companies and as a country are online, and so it ought to be secured in a way so people can't steal our innovation, our identities, information about our children. So encryption is a very good thing, and the FBI has long said that.

The challenge we face is that we never lived in a world with locks that couldn't be opened on a judge's order, and so now we face that world where all of our lives will be covered by strong encryption and so a judge's orders under the Fourth Amendment will be unable to be complied with, and there are significant costs to that. That's what I meant by the conflict of the values, public safety and security on the Internet, and that's what makes it such a really hard problem.

Mr. CONYERS. Thank you.

Over the summer we received reports that a single engine Cessna operated by the FBI and mounted with surveillance equipment had flown multiple times over metro Detroit, including two lengthy flights over Dearborn where many citizens feel reason to distrust the FBI because of their religious or ethnic background. You've been forthcoming to my staff about some of the details of this program. Can you give the public a similar overview here?

Mr. COMEY. Sure. I'd be happy to, Mr. Conyers.

When we investigate criminals or spies or terrorists, a key tool is surveillance, to follow them. We follow them a lot in cars. We follow them on foot. There are plenty of circumstances where both of those options don't work real well, and so since the Wright brothers, we have used airplanes to follow people in our investigations. If a spy is going out to meet somebody and it's an area where we can't park cars, we'll sometimes try and get a small plane up to be able to get eyes on that meet with their contact.

And so it's a feature—and I hope this doesn't shock the American people, I think I should be in trouble with them if we're not doing this—we use planes in our predicated investigations to conduct surveillance of people who are under investigation. We do not use planes for mass surveillance.

And so the good folks in Michigan who saw a plane in the air, I think a lot of them had a chance to meet with my SAC out there and have him explain, look, this is what we do in criminal cases.

It should make sense if you understand how we use it in individual cases.

So we have a small number of airplanes—I actually wish we had more—that we use to follow people in places where it's hard to follow them on foot or in a car.

Mr. CONYERS. Thank you for your response to my questions.

Mr. GOODLATTE. Thank you.

The Chair recognizes the gentleman from Virginia, Mr. Forbes, for 5 minutes.

Mr. FORBES. Mr. Chairman, thank you.

Director Comey, thank you, not just for being here, but for your service. I also want to thank all of your staff. I know the dedication they put into serving this country, and we appreciate them being here.

If my friend Steve Chabot were here, he would also commend you for your selection of William and Mary as an undergraduate. And I will tell you that if we couldn't convince you to go to the University of Virginia Law School, Chicago was probably a good second choice.

But I have a question. As I listened to the Ranking Member today talk about trust, and he talked about the symbols that you have on your desk regarding police brutality and efforts by law enforcement, but you mentioned it was important to have reality and perception, both of those, when you're looking to that trust.

Tell me the symbols if you would, because what he raised was important, but tell me the symbols on your desk or in your office that would give me comfort in knowing that there was also a perception that you were equally looking at organized groups that were coming into areas like Ferguson and Baltimore to foment unrest, especially groups that were outside those communities and especially those groups who might be impacting violence against law enforcement. Because as you mentioned, there are two curves, not just one curve.

Mr. COMEY. Thank you, Mr. Forbes.

First of all, to make sure the record is clear, what I have on my desk to me is a message of the importance of restraint and oversight within government. And so it's just—it's a wiretap order that relates to Martin Luther King. It's not about police misconduct, which is something—obviously, police misconduct is something we take very seriously.

I've devoted my whole life to law enforcement. I come from a law enforcement family. One of the things that's prominent in my office is a picture of my grandfather in 1929 escorting a dangerous felon to jail. My grandfather was a detective who rose up to lead a significant police department. And so I care an awful lot about making sure law enforcement has the confidence of the community, that we conduct ourselves well, but that we protect law enforcement from attacks.

One of the things in my office that reminds me of this is my phone. Whenever a police officer is killed in the line of duty, I call the chief or sheriff of that slain officer to offer the condolences of the FBI. I make far too many phone calls.

And so we care about both, making sure law enforcement acts well and that we investigate people who would harm law enforce-

ment, whether it's groups, sophisticated groups, or individual actors. It's a feature of all the work that we do.

Mr. FORBES. And, Director, I would ask that at some point in time you could submit for the record the data you have on these outside groups that are coming into these communities when we have situations like this who might be stirring up unrest and especially activity against law enforcement; and also any data you have regarding the impact or even the numbers of gang members that might be currently being released by the government who might be here illegally, because when we ask those questions of Homeland Security, they can't give us any of that data.

The second question I'd have for you, as you know, the OPM breach impacted over 22 million current, former, and prospective Federal employees and contractors. Considering these individuals use personal e-mail accounts for their own personal communication and store private information relating to financial transactions, their children, and health care, do you think the OPM breach has made these individuals more vulnerable to social engineering tactics used by hackers? And in what ways could encryption enhance the security of personal information of those who have had their information compromised during the OPM breach?

Mr. COMEY. I think the OPM breach, as I've said in other settings, is disastrous because it's a gold mine for foreign intelligence services that would allow them to use that material to conduct very sophisticated socially engineered spear phishing attacks, for example, to penetrate people's systems.

I think encryption is very important to protect people's information. I don't think encryption will directly blunt that particular vector because it would allow a nation state to send me an e-mail from my sister about my nephew with an attachment, and it's highly likely I will open that e-mail and click on that attachment. So I actually see them as two separate problems, both serious problems, though.

Mr. FORBES. Good. Thank you, Mr. Director.

And with that, Mr. Chairman, I yield back.

Mr. GOODLATTE. That Chair thanks the gentleman and recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

And thank you, Director Comey, for being here again.

The National Instant Background Check System was created as a result of the Brady Act of 1993, before I was in the Congress, and it requires that gun sales by licensed gun dealers are subject to background checks but allows transactions to proceed after 3 days unless the FBI stops the transaction based on criteria such as felony record or domestic violence, misdemeanor convictions, and the like.

Now, under the rule, even if the FBI has not completed its check, the dealer has the discretion to complete the sale after 3 days have passed and they haven't received a red light from the FBI.

Now, it's my understanding from news reports that the man who shot and killed nine people at the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, on June 17 was sold the gun by a dealer who waited 5 days but did not receive a response from the NICS examiner. Now, the shooter had a drug pos-

session conviction that, if it had been found by the NICS examiner, would have prevented the gun sale. Due in part to an error in the shooter's arrest records and also the large caseload and time constraints placed on the NICS examiner, the gun dealer didn't receive the red light that would have prevented this gun sale and possibly prevented this massacre.

So I have a couple of questions. First, what can be done to make sure that we have a timely response and we have the data available to prevent the sale of guns to those who are not eligible to buy them, number one? Number two, should the law require a green light from the FBI to prevent a firearms transfer to those prohibited by law from buying them instead of the red light system that we have now? And do you think that we should examine the amount of time that we give for background checks beyond 3 days if we don't go to an affirmative green light system?

Mr. COMEY. Thank you, Ms. Lofgren.

With respect to the case of Dylann Roof, as you said, dealers must wait 3 days, business days, to give the FBI an opportunity to conduct a background check. In that circumstance the gun dealer was notified it was in delayed pending status; and at the end of 3 days, if it's still in delayed pending, the gun dealer has the discretion to transfer or to wait. Some large gun dealers wait. This gun dealer transferred, which was consistent with the law. And there were a number of errors in the processing of his that allowed his drug possession arrest to be missed, and so the gun was transferred.

We have stared very, very hard at that and have tried to figure out what we can learn from that. There were some easy fixes to our processes, but we are looking at bigger fixes to see whether we can surge resources, whether we can add innovation to make our processing faster.

But the other key piece is going to be we must get better records from our State and local partners so that when our examiners query a database they have the disposition reported and they don't have to go tracking it down. We're having lots of productive conversations with State and local law enforcement who see in the wake of the pain of that tragedy the importance of giving us those records. So that's what we're doing to try and improve our processing.

The policy questions are really not for the FBI. We comply with the law as it stands today, which is we have 3 days to get it done. We'll do our best to get it done in 3 days. If Congress were to change that, we would comply, obviously.

Ms. LOFGREN. All right. Getting back to encryption, I understand the concerns that you've used raised here today and in the past, but the experts really say trying to get a back door is a mistake. I mean, all the way from the inventors of public key encryption, people like Whit Diffie, who did a very excellent report from MIT, if you have the back door the hackers will get it and China will get it and we will be less safe.

So that leads me to a question about the use of encryption by the FBI. Are you encrypting all of your data about your FBI agents and your personnel and your payroll and all of your systems?

Mr. COMEY. We do not encrypt all of our data. We use encryption on a significant amount of our data. I'd have to follow up with you to give you the particulars on maybe a percentage breakdown. It's an important feature of our work.

Ms. LOFGREN. I'd like to follow up with that because I was stunned that the Office of Personnel did not have important data that encrypted. The Federal Government should protect itself by encrypting this data. We know that we're being hacked constantly by state actors and enemies of our country, and I'm sure that they would love to get data about the FBI as well, and I look forward to hearing greater details on that.

And I yield back, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentlewoman and recognizes the gentleman from California, Mr. Issa, for 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman.

I've got so many questions and so little time, so I will try to touch on each of them, and bear with me. On Stingrays I'm going to ask you to tell us now or for the record how you control the access to these products when they're not being used, how you control them when they are being used, not just at the FBI, but to the extent that you're cooperating with non-Federal agencies around the country that have these devices.

And specifically I'm very concerned that since they're being used at times without warrant, almost mostly, and there are at least some allegations they've been used to track policemen's girlfriends' or wives' activities and so on, that they are too powerful a tool not to have a series of controls. And I'd like to—again, some of this you can answer for the record—I think on that I'd like to have a full understanding of Federal policy and controls.

In the case of encryption, I'm only going to ask you, it will be a long answer, provide for the record, any and all studies you have to show the value of encryption and the value of your access or ability to not go dark. And if it's classified, I'll look at it in a classified session, but I'd like to fully understand the value and the studies related to that general direction of the Administration.

But I'd like to take up for today more a question on some historic pieces. A few offices away they're dealing with Secretary Clinton, so I won't ask about those today. I think that's certainly an ongoing investigation as to her use of private e-mail for transmitting what turns out to be sensitive information.

But in the case of late 2011, well before your tenure, Solyndra went bankrupt after accepting half a billion dollars in taxpayers' money. At that time we began an investigation in an adjacent Committee, the Oversight Committee, and we were told by the DOE inspector general that he could not talk to us because the FBI at that time had an ongoing investigation.

It's now 4 years later, and the Department, the IG did release information, but we have not received any indication from the FBI. So today I'd like to ask you who at the FBI made decisions not to bring any charges against Solyndra executives and what the basis was to find no fault in that loss of $500 million, and particularly since there was evidence provided publicly by our Committee that there were emergency efforts to get them additional money to try

to have their bankruptcy delayed. And that was done by Federal employees, including a gentleman named Jonathan Silver.

You might remember that in May in 2013, the President stood beside the Attorney General and declared that there would be serious investigation by DOJ and FBI into the political targeting done by the IRS. Months later the President declared there wasn't a smidgeon of corruption related to the IRS.

Director, you know that, in fact, there was targeting. The evidence is convincing. Where do you stand on bringing accountability to those involved at all levels to targeting conservatives and pro-Israel groups by the IRS, including but not limited to Lois Lerner?

Mr. COMEY. Thank you, Congressman.

With respect to the first two, the Stingrays and the encryption, we'll get you information for the record.

With respect to Solyndra, first of all, just to clarify something, the FBI doesn't make decisions to prosecute. We investigate, bring the evidence to prosecution.

Mr. ISSA. And I appreciate that, but there is either a decision to refer for prosecution or not. And to the extent that there was one, I would like the evidence that it was referred but not prosecuted. To the extent that there was a decision not to refer one or more, that would be helpful. I appreciate that the other part of Justice handles the other part, and we will have the Attorney General here shortly.

Mr. COMEY. Got you. We worked the Solyndra matter, we, the FBI, very, very hard and had it reviewed by two different U.S. attorney's offices, one in California, one in New York, who both made the same decision, that there was insufficient evidence to bring prosecutions. I'm probably limited in what I could say about the details of it here because it was a grand jury investigation, but that's the upshot of it. I had a lot of folks worked it very, very hard. One U.S. attorney's office looked it. I asked that it be brought to a second U.S. attorney's office, my alma mater, the Southern District of New York. They took a look at it and decided there was insufficient basis to prosecute criminally. And so that's where the matter stands.

With respect to the IRS investigation, I think as I sit here it's still pending, and so I am not able to talk about it in any way because it's still a pending investigation.

Mr. ISSA. Mr. Chairman, I just want to close with a very short comment. It was 2010 when we became aware that the IRS was targeting conservatives. It's now 2015, almost 2016. I really would appreciate if the FBI would come up with a time line that says an investigation is not ongoing and aggressively pursued if a certain period of time passes and nothing has happened. I would only ask that 5 years begin to become an amount of time in which the FBI can say: We can't say with a straight face it's ongoing if it's 5 years later and nothing has happened.

Thank you, Mr. Chairman.

Mr. GOODLATTE. Thank you.

The Chair recognizes the gentleman from Tennessee, Mr. Cohen, for 5 minutes.

Mr. COHEN. Thank you, Mr. Chair.

First, I want to welcome you. I'm a big fan of yours. But at the same time I would like to ask you a question. I understand you keep a copy of the FBI's request to wiretap Dr. Martin Luther King, Jr., on your desk as a reminder of the FBI's capacity to do wrong. Is that correct?

Mr. COMEY. That's correct.

Mr. COHEN. I commend you for that.

That occurred during J. Edgar Hoover's tenure as Director. As you know, J. Edgar Hoover did some awful, terrible things in his life and as FBI Director. He started the COINTELPRO. I might be mispronouncing that. How do you pronounce that?

Mr. COMEY. I think you got it, COINTELPRO.

Mr. COHEN. COINTELPRO program, which harassed civil rights workers, SNCC people, SCLC people, Dr. King in particular, others, political activists and homosexuals. He was abusive. He was the opposite of justice. His efforts to silence Dr. King and out homosexuals working for the Federal Government were deplorable and a stain on our Nation's history and on the FBI.

It's been reported that at one point he even had a letter sent to Dr. King threatening to expose all kinds of private information collected surreptitiously. The letter appeared to suggest that Dr. King should kill himself to save himself from embarrassment. "King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do it. You are done. There is but one way out for you. You better take it before your filthy, abnormal, fraudulent self is bared to the nation." This was the head of FBI.

His treatment of homosexuals was no better. He called them sex deviants. He ordered the FBI to undertake extraordinary efforts to identify everyone in the Bureau who was even suspected of being homosexual in the Federal Government.

There's a documentary been done on this, it's on Yahoo.com, by Michael Isikoff called "Uniquely Nasty." I encourage you to watch it. I watched it and was shocked. It premiered at the Newseum. It's sickening what the FBI did.

In 1951, Hoover issued a memo to top FBI officials saying each supervisor will be held personally responsible to underline in green pencil the names of individuals who are alleged to be sex deviants. This was discovered through a FOIA effort 2 years ago. The FBI eventually collected more than 360,000 files on gays and lesbians.

It's reported in 1952 he outed a young campaign aide, a Vandenberg, Jr., and went on a war on him. And Senator Vandenberg, a Republican, eventually committed suicide in the Senate office because of what they brought out about his son and what they were doing to destroy him.

J. Edgar Hoover was a man that doesn't reflect the good people of the FBI or reflect what you and the FBI are trying to do today. The FBI's own Web site declared the COINTELPRO program, as rightly criticized by Congress and the American people, for breaching First Amendment rights and other reasons, yet his name continues to adorn the FBI building.

Would you agree that his name is not appropriate as a reflection of what the fine people at the FBI today try to do to bring about justice in our country?

Mr. COMEY. I'm sorry, Hoover's name?

Mr. COHEN. Yes, sir.

Mr. COMEY. I am not following the question.

Mr. COHEN. I'm saying does it not reflect the qualities that the FBI individuals and the FBI today have in pursuing justice and being fair and not using tactics to attack minorities in this country?

Mr. COMEY. I see. Thank you. I'm sorry. The FBI today is vastly different than it was under its first Director in some of the ways you mentioned and in lots other ways. I keep that under the glass of my desk, not to dump on Hoover—I never knew the man—but to make sure people understand the danger in becoming—in falling in love with your own view of things and the danger in the absence of constraint and oversight.

I am somebody who believes people should be very skeptical of government power. I'm a nice person. I suppose you should trust me, but you should oversee me, and I should be checked, and I should be balanced. That's the way you constrain power. It's there to remind me.

Mr. COHEN. Yes, sir. And I agree and I appreciate that, but do you agree that his name is not reflective of the what the FBI stands for and what the FBI agents of today believe in and do?

Mr. COMEY. I think that's fair if you're focusing on—I mean, Hoover did a lot of good things for law enforcement in the United States, did a lot of things that, through the lens of history, we reject as improper, and so you—I'm no historian, but I would imagine a historian would say you've got to take the total measure of the person to figure out what's bad and what's good. I'm just not equipped to do that.

Mr. COHEN. Thank you, sir. I would like to see his name taken off the building, and I have bill. Representative Burton had it with Chris Shays in the past, and I'm going to reintroduce that bill, but I was hoping, as I mentioned to you the last time, that when we have a new building some time in the future, it's named for somebody like you.

Mr. COMEY. Well, I appreciate that. I hope it's not.

Mr. COHEN. Or Congressman Edwards or Attorney General Kennedy.

And I yield back the balance of my time.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Iowa, Mr. King, for 5 minutes.

Mr. KING. Thank you, Mr. Chairman.

Director Comey, thanks for coming to testify, and I just would comment that I appreciate your response. So when you use the reference "the lens of history," there is a different set of values that applies today than applied back in those days. But I'm looking at our values today, and I'm watching as there is a fairly strong push here for sentencing reform in the United States. And I've watched as the President or the Administration, at least, has directed that thousands be released onto the streets before they serve their terms and that we've seen that some of them have been charged with homicide and found guilty of homicide. I think that number is around 121 or so, but I thought I saw the number 36,007 felons released and then a subsequent number.

I'm actually blurred by the parade of releases that we've seen, and now I see it appears to be a group of legislators that believe we can save us some tax dollars by releasing more onto the streets.

Are you aware of any studies that would help us quantify the impact of these releases in terms of either prospective crimes that are likely to be committed or perhaps even quantifying it in terms of the dollar value as that's suffered in great huge whopping chunks by crime victims?

Mr. COMEY. I'm not aware of any studies on that. It's not that I would be. That's sort of a policy question, but I'm not aware of any.

Mr. KING. They're very hard to find. I've searched a long ways back. I'm only going from memory. It occurs to me that in 1992 there was a Justice Department study that did quantify numerically the cost of crime, but you have any studies that show statistically whether there would be more crime or less crime that would take place because of the releases, the early releases?

Mr. COMEY. I'm not aware of any studies on that.

Mr. KING. What would be your professional estimate? I don't need a number. Would we have more crime or less crime?

Mr. COMEY. Well, I know we face, as a country, a significant challenge with recidivism, a high re-offend rate among people who are released, and my whole career is dedicated to the proposition that law enforcement contributes to a drop in crime. It's certainly not entirely responsible for the historic drop in crime we've seen over in my lifetime, but it's a big part of it, and so that's the way I think about it.

Mr. KING. Mandatory sentencing statistically shows to have had a positive impact on reducing the crime in the streets of America?

Mr. COMEY. I think so. Mandatory minimums have been an important part of my work as a prosecutor. Reasonable people can discuss whether it should be at this level or this level, but some mandatory sentence, some fixed prospect of punishment is very, very valuable in incapacitating people and in developing cooperators.

Mr. KING. And some time back I sat down with a very impressive chief of police of one of our major cities who remarked to me about the high, the very high homicide rate in the inner city of his city, and his response was that the Black-on-Black homicide rate in that city was roughly 98 percent of the homicides that took place.

I don't know that we discuss these kind of statistics, and I'd be hopeful that we could find a way to do this and alleviate this situation that we have. I'd just say we've done into a void on this for a politically correct reason, but are you aware of any data that would reflect what I represented to you?

Mr. COMEY. I think there's a lot of data collected by criminologists and others on the demographic component—excuse me, the demographics of homicide victims and perpetrators. I can't cite it to you off the top of my head, but I know there is smart people that have done that work.

Mr. KING. And that 98 percent number, that wouldn't be shocking to you if that were proven out to be true by a legitimate study?

Mr. COMEY. I don't think it would shock me in particular neighborhoods that are heavily concentrated with people of a certain de-

mographic background, but I don't know the number off the top of my head.

Mr. KING. Yes, thank you. Is there an investigation of Planned Parenthood currently taking place in the FBI?

Mr. COMEY. I know, Congressman, as I sit here, I'm not able to answer that question because I don't know enough. I know there's been letters written to the Department of Justice about it. I'll have to get back to you on that one because I don't know the status of matters within the FBI on that, sitting here this morning.

Mr. KING. Has anyone from the Administration, to your knowledge, ever sought to influence you or any of your subordinates on whether or not to investigate a crime?

Mr. COMEY. Never.

Mr. KING. And specifically not Planned Parenthood either would be included in that?

Mr. COMEY. That would be included.

Mr. KING. I thank you. That would be consistent with your competent, independent, and honest characteristics of the FBI. I'd just pose this question that—let me quickly go another way. USA FREEDOM Act, you're implementing it now, and do you have access to more or less information than you had before the USA FREEDOM Act was passed?

Mr. COMEY. It really hasn't changed because we're still under the old telephone metadata system. As I said to the Chairman, I think the new one kicks in at the end of November, so currently our world is unchanged.

Mr. KING. Okay. Do you expect more or less?

Mr. COMEY. I expect more, actually.

Mr. KING. That would be interesting to follow up on if I had another minute, but I will yield back and thank the Chairman.

Mr. GOODLATTE. The gentleman does not have another minute.

But the Chair will recognize the gentlewoman from California, Ms. Chu for 5 minutes.

Ms. CHU. Director Comey, I want to discuss with you a series of very troubling Federal investigations against Chinese American scientists, who are treated as spies, have their lives turned upside down, only to have all the charges dropped.

Most recently, we have a case of Dr. Xi Xiaoxing, an American citizen and well respected professor who was a chair of the Physics Department at Temple University.

He led a normal and peaceful life as a scientist, professor, and researcher with his two daughters and a wife in a quiet Pennsylvania neighborhood. He had no criminal record, no history of violence, just an average American in academia. But one day, at the break of dawn, about a dozen armed FBI agents stormed into his house with their guns drawn. He was handcuffed in his own home, and his two young daughters and wife in pajamas and directed outside of the house at gunpoint. The stated charge, wire fraud. However, in the interrogation, it was clear he was being accused of being a spy for China.

Since then, his life has been turned upside down. He lost his title as chair of the Physics Department. His reputation was irreparably damaged. His wife endured psychological and emotional trauma, as

does his own whole family and himself, of course. And after all of this, the charges against Dr. Xi were dropped.

My understanding of cases of wire fraud is that generally people aren't even handcuffed, let alone arrested or paraded in font of their family or neighborhood as criminals at gunpoint. Rather, they've been given an opportunity to self-surrender, and if someone is being investigated for wire fraud, they are usually informed about such an investigation in a target letter.

But we know that Professor Xi is not alone. Sherry Chen was also recently arrested, a U.S. citizen, an employee of the National Weather Service in Ohio. She was arrested at her place of work, led in handcuffs past her coworkers to a Federal courthouse 40 miles away, where she was told she faced 25 years in prison and a million dollars in fines. Several months later, all the charges were dropped without any explanation.

This is reminiscent, of course, of Dr. Wen Ho Lee another U.S. citizen whose life was ruined when he was accused of being a spy for China, only to have 58 of the 59 charges dropped.

Let's not forget that during World War II, 120,000 Japanese Americans lost everything they had and were imprisoned in desolate camps because they were accused of being spies for Japan. Three-quarters of them were U.S. citizens. Seventy years later, not a single case of espionage was proven. I'm particularly concerned about this because there is a stereotype that Asian Americans are perpetual foreigners, no matter how long they've lived in this country.

So my question to you is, is this common practice to have a dozen armed FBI agents arrest someone for wire fraud, someone who is not a flight risk and poses no harm to law enforcement, or is there a presumption of guilt went it comes to Chinese Americans because they are viewed as spies for China?

Mr. COMEY. Thank you, Congresswoman.

At the outset, the challenge—I'm going to answer. The challenge for me in answering is I can't talk about the facts of something that is of an investigation, including ones that are pending.

I guess I can say this. First of all, we operate with no presumption that anyone is guilty or any stereotype about any particular person. We are a fact-based organization. We are required to gather facts and then, through a prosecutor, present them to a judge to make a showing of probable cause before we can get a warrant to arrest anybody.

A whole lot of people in this country are arrested on wire fraud charges. I've been involved in many cases where people were handcuffed and arrested because wire fraud is a very serious felony. The particulars of the case I can't talk about it, but I would not connect the dots in the manner that you have, and that's probably all I can say about individual matters.

Ms. CHU. Well, we understand that the threat of economic espionage is real, and we do not take it lightly. However, we want to make sure that in all cases, there is due process and that otherwise innocent Americans do not become suspicious simply because the person taking those actions have an ethnic surname.

Yet in the case of Professor Xi, his investigation came out of the blue. He had no idea he was being investigated, primarily because he did nothing wrong, as evidenced by the dropped charges.

Do you know how many Chinese Americans are being surveyed?

Mr. COMEY. I do not.

Ms. CHU. Well, I will personally follow up with you on this issue to figure out what is happening in cases like Professor Xi's and how we can make sure that no other American, regardless of their origin or background, endures this kind of egregious humiliation and shame.

And, with that, I yield back.

Mr. GOODLATTE. The Chair thanks the gentlewoman and recognizes the gentleman from Texas, Mr. Gohmert, for 5 minutes.

Mr. GOHMERT. Well, Director Comey, thank you for being here. I don't think I ever told you, but back in July-August timeframe of 2007, I was talking with a powerful Democratic Senator, and we agreed that you had a great reputation for justice, honorable man that would potentially be a good Attorney General. It ended up being Mukasey, but you were discussed very favorably by both sides of the aisle, people unlikely to be talking, but we appreciate your work.

I want to touch on something my friend Steve King brought up. I know there's a lot of talk about how we need to have reform and people being released from prison, but as someone who has worked with the system, you prosecuted, I prosecuted, I've been a judge, I've been court-appointed to defend, and isn't it true that some people that actually plead to nonviolent offenses do so as part of a plea agreement where the prosecutor drops a gun charge or some charge of violence in order to get a plea in the case and a lesser sentence, haven't you seen that happen?

Mr. COMEY. I've seen that happen.

Mr. GOHMERT. Yes. And so that's why for someone like me, who's a former judge, who saw those kind of plea agreements take place, even though I was in the State side, it's shocking to see people come from the outside and say this wasn't a fair sentence without really considering what could have been prosecuted, what could have been pursued, and what was, you know, a transaction or an agreement between a prosecutor and defense attorney that the judge considered all the circumstances and came down on the side of the agreement.

Now, I want to touch on something else you had said about with Iraq refugees, you had a database, apparently, of fingerprints from IEDs, evidence that had been obtained from Iraq. Did I understand that correctly?

Mr. COMEY. Yes, sir.

Mr. GOHMERT. Now, with regard to the masses of Syrian refugees, I'm not aware of a lot of IEDs evidence we've gotten from which you could get fingerprints. Is there such a database?

Mr. COMEY. I think that's right. There may be some and a variety of other intelligence sources that may help us try and understand who people are, but the point I was trying to make is we had a whole lot more information about Iraq because our soldiers had been there.

Mr. GOHMERT. Right.

Mr. COMEY. Run into people and collected information.

Mr. GOHMERT. Well, and that goes to a concern of mine. I'm not the biggest fan of the U.N., but they have data pulled from their Web site this morning that says—starting off at more than 43 million people worldwide are now forcibly displaced as a result of a conflict and persecution, and it goes on to say that children constitute about 41 percent of the world's refugees, and about half of all refugees are women.

So it was very disturbing to pull this from the U.N. Web site in September that says of the 381,412 arrivals that came across the Mediterranean sea just this year, up to September, that 15 percent were children, 13 percent were women, and 72 percent were men, and then when you take that along with our DNI James Clapper saying that this provides a prime opportunity for Islamic State groups to attack Western targets—he said, "It's a disaster of biblical proportions"—and then you take statements that have been made by ISIS leaders themselves that they have been able to place more than 4,000 warriors in with the refugees, this inordinate number of men, has that spiked concern in the FBI, along with what you've testified before about ISIS having people in every State?

Mr. COMEY. Yes, sir. It's a risk that we are focused on and trying to do everything we can to mitigate.

Mr. GOHMERT. But without a good fingerprint database, without good identification, I mean, how can you be sure that anyone is who they say they are? You don't have fingerprints to go against it. They've got documents that say they're one—I've been there on the border when I've watched people exchange identification information and decide to use the other ones. Is there a good way to avoid that that the FBI is able to use?

Mr. COMEY. The only thing we can query is information that we have, and so if we have no information on someone, they've never crossed our radar screen, never been a ripple in the pond, there will be no record of them there, and so it will be challenging.

Mr. GOHMERT. Thank you. My time is expired.

I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Illinois, Mr. Gutierrez, for 5 minutes.

Mr. GUTIERREZ. Thank you, Mr. Chairman.

And welcome, Director.

I'm just going to ask you to have a conversation about one area, and that's about guns. In my hometown, there could be 40, 50 shootings in a weekend. That's about a whole classroom of kids any weekend. And so I know that you have a relationship with making sure that we check who can and cannot purchase guns here at the FBI. And it just seems that whatever we do in Chicago, guns are just—well, first, our laws have been weakened because there have been challenges to them, so we used to have pretty strong—when I first got elected in 1986 to the Chicago City Council, they give you a badge in Chicago, and you can get a gun. I opted not to take the badge or the gun. I figured the Chicago police could do both of those things, wear the badge and carry the gun for me and for the rest of the people, and I think the people of the city of Chicago were well served by me making that decision.

But, look, so here we have like a majority in the Congress of the United States that's really unwilling to take up the challenge that guns and firearms are—and they're coming from Indiana, and they're coming from Mississippi, and they're coming from all over, and they wind up in Chicago. So I guess, if you could just tell us, what are you ideas on how do I and people at a local level or as a Member of Congress, how do I help curb gun violence? What things can we do to help curb, absent legislation?

Mr. COMEY. Well, the FBI's business is not policymaking; it's enforcement of the law. And so we spend a lot of time trying to reduce gun violence through aggressive enforcement. It's a crime for a felon to possess a gun in this country; for a drug addict; for a drug dealer; for someone who is convicted of a domestic violence misdemeanor to do it; to use it in crime of violence. And so I've devoted a lot of my career as a prosecutor—and the FBI does investigating—to impose cost to change behavior so the bad guys don't have a gun on their waistband. And that means more fistfights, maybe more stabbings, but fewer shootings because the challenge we face in a lot of cities is the bad guys think it's just another a piece of clothing. So they think about as much about the gun as they do about their socks, and that leads to a whole lot more shooting based on people bumping into each other, frankly.

And so our mission is to try and send a strong message of deterrence that you ought not to have that gun, you ought to think a lot more about the gun than your socks, and that will make that corner safer. But it requires tremendous effort by the law enforcement community. We're doing a lot of that, though, including in Chicago, where your characterization is exactly right.

Mr. GUTIERREZ. Could you tell us, the Members, what kinds of things are we doing in Chicago via your agency and the Federal Government to help the people of the city?

Mr. COMEY. Well, in Chicago, we have actually gone so far as to put FBI agents with Chicago police officers in squad cars to try and focus on some of the predators who are driving this violence, the gang bangers who think that they operate freely. So we do gang task forces. We do drug task forces. And as I said, we operate even on an ad hoc basis to try and lock up some of the repeat offenders. And the idea there is to try and change behavior by ripping out the worst and convincing the rest you should not have a firearm with you if you are a prohibited person.

Mr. GUTIERREZ. So as I look at the challenge of gun violence in the city of Chicago and I see that there are—I mean, if we took a map of the city of Chicago and we put, reluctantly, little stars where people had been murdered due to gun violence, do you know or have you seen, is it the whole city of Chicago? When I look at it, I'm not that worried about my grandson walking in Portage Park to the park. I'm worried but not that worried as I would be in other neighborhoods of the city. So what other dimensions are there that relate to gun violence as you've seen from a——

Mr. COMEY. I know the city of Chicago pretty well, having gone to law school and been there many, many times. And the story of Chicago is a lot like the story of a bunch of cities around the country. It's localized. The violence is heavily concentrated. Chicago, primarily south, some west, obviously. And it is groups of primarily

young men who are carrying firearms when they're prohibited by law from carrying them on the streets, and that inevitably leads—all human encounters ratchet up to the most serious available weapon. And so what would have been a fistfight when you were a kid, today is a shootout because the gun is there. And what we in law enforcement are trying to do is change that behavior. These kids may not be well educated, but they are very good at cost-benefit analysis. And the idea is to force a cost-benefit analysis. That gun should be a huge liability in the eye of that felon, that drug dealer, that drug addict, and that's the way we hope to change behavior.

Mr. GUTIERREZ. Mr. Director—just 15 seconds, and I'll finish up, Mr. Chairman.

So Mr. Director, there are a group of us in the Hispanic Congressional Caucus and African American Members of color, we like to have a roundtable discussion with you, a conversation from different parts of the United States and not in such a formal setting as this in which you might be able to share with us how better, in communities of color in America, where the gun violence is so rampant, you might give us some of your thoughtful input. Would you agree to do that with us?

Mr. COMEY. I'd be happy to.

Mr. GUTIERREZ. Thank you so much, Mr. Director.

Mr. GOODLATTE. The Chair recognizes the gentleman from Texas, Mr. Poe, for 5 minutes.

Mr. POE. Thank you, Mr. Chairman.

Mr. Director, thank you for being here. I'm going to talk about several subjects, see how many of them I can get in in 5 minutes.

I first want to talk about ECPA, the idea that under current law, that if e-mail is stored in the cloud, government doesn't need a warrant to obtain that e-mail. Is that your understanding of the law?

Mr. COMEY. I think the law is—and you probably know best than I, but I think it's after 180 days.

Mr. POE. Yes, after 180 days.

Mr. COMEY. Right. We still operate under a warrant, the FBI does, that's just our policy, but I think that's the law. If it's older than 180 days, it can be gotten through other legal processes.

Mr. POE. And thanks for your clarification. It's after 180 days. Before 180 days or during 180 days, you got to have a warrant, no matter who you are. FBI policy is, though, you still get a warrant if it's over 180 days?

Mr. COMEY. Correct.

Mr. POE. But other government agencies still have the ability to seize that e-mail without a warrant. Law enforcement. I mean, it could be a local law enforcement, the city police, sheriff's department, other law enforcement can seize that e-mail in their jurisdiction because the law doesn't require they get a warrant. I mean, is that your understanding of the law?

Mr. COMEY. They would need some kind of legal process. They couldn't just walk in and take it, but my understanding is the law would permit them to get it through a subpoena or some other court order short of a warrant.

Mr. POE. That's right. So they don't need a warrant. They need some other court document from a magistrate, if so. And I'm sure you're aware that myself and Ms. Zoe Lofgren filed legislation to require any law enforcement agency, any government agency to obtain a warrant if e-mails are over 6 months old stored in a cloud. You aware of that legislation?

Mr. COMEY. I am. I'm generally aware, yes, sir.

Mr. POE. Okay. Next subject, 702, talk about obtaining backdoor information from different companies such as Google or Yahoo or whoever. Does the act, the FBI request that a backdoor device be put into like a cell phone?

Mr. COMEY. I don't know what you mean by backdoor device.

Mr. POE. Well, where the FBI could obtain the information in the cell phone without a warrant and ask the maker of the phone, for example, to install a device in the phone to obtain that information.

Mr. COMEY. Oh, I see. No, we would need a court order to be able to either in a device or online to be able to take content or implant something in a phone, not just a warrant. We need a title III order or a FISA court order.

Mr. POE. My question, though, is does the FBI request—and it may be that you don't—manufacturers to put a device in the phone itself to obtain that backdoor information, to have it available and then a warrant obtained?

Mr. COMEY. No.

Mr. POE. You don't request that?

Mr. COMEY. Nope.

Mr. POE. Okay.

Mr. COMEY. No, when we collect information, it's pursuant—we're talking about the content of people's communication or what they've stored on a device, we do it through a court order. We don't do it through asking someone who made the device to give us access to it voluntarily.

Mr. POE. Okay. When you say court order, are you talking about a warrant or some other type of court order?

Mr. COMEY. Right. Either a search warrant from a judge to open a locked device or an order from a Federal judge either in a national security case or a criminal case if we're looking to intercept communication as it's moving.

Mr. POE. I think that, you know, the Fourth Amendment applies to that type of procedure, and you're saying the FBI complies with the law, the Fourth Amendment, on obtaining that information?

Mr. COMEY. Yes. The Fourth Amendment is part of this sort of the spine of the FBI.

Mr. POE. It's the what of the FBI?

Mr. COMEY. The spine of the FBI.

Mr. POE. I am glad to hear that. Let's talk about the surveillance with the use of drones and fixed-wing aircraft. Specifically, targeted surveillance with the use of a drone, does the FBI obtain a warrant to do that, use of a drone, fixed-wing aircraft or drone, whichever you want to call it.

Mr. COMEY. Any kind of aircraft, we don't. If what we're doing is, which is what we used them for, we have a pilot fly around and follow somebody. Drones, we don't. We have a small number of unmanned aircraft. We may use them for fixed surveillance, like

when that guy had the kid in the bunker in Alabama, we used a drone to go over the top because we were afraid he would shoot one of the pilots. We had unmanned aircraft. We operate drones within line of sight.

Mr. POE. Okay.

Mr. COMEY. So when we're talking about surveilling someone, we're really talking about an airplane with a human being in it flying them around. We do not get a warrant for that. The law doesn't require it, but that's not involved with collecting the communications of somebody.

Mr. POE. I understand. I'm not talking about exigent circumstances. I'm just any circumstance, the law doesn't require—or there is no law saying the Fourth Amendment applies to the use of drones. The FAA makes those decisions. Does it not?

Mr. COMEY. Right. To follow somebody in a car or on foot or in a plane, we have to have a predicated investigation, but we don't have to go to court to get permission to follow that person.

Mr. POE. Do you think the FBI ought to make the rules regarding protection of the Fourth Amendment, or should Congress weigh in on what reasonable expectation of privacy should be regarding that type of issue?

Mr. COMEY. The FBI doesn't make any laws. Congress makes the laws, and the courts interpret them.

Mr. POE. I didn't say the FBI. Reclaiming my time, if the Chair would be so patient. The FAA—F-A-A, not the F-B—I—.

Mr. COMEY. I misunderstood.

Mr. POE. Not the F, B, and I, the FAA may make the regulations on what you can do with a drone and what you can't do. I think that Congress ought to weigh in and determine what the reasonable expectation of privacy ought to be with the use of drones.

Do you have an opinion on that, being the Director of the FBI? Do you want the FAA to continue to do it, or do you think Congress ought to set that standard?

Mr. COMEY. I don't think I have——

Mr. GOODLATTE. The time of the gentleman has expired, but we'll permit the Director to answer the question.

Mr. COMEY. I don't think I have a view or a preference. I mean, the FBI, we are maniacs about wanting to follow the law.

Mr. POE. I understand.

Mr. COMEY. So if Congress decided to change the law, we would follow it.

Mr. POE. Thank you, Mr. Chairman.

Mr. GOODLATTE. The Chair recognizes the gentleman from Georgia, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Director Comey, in your testimony, you mentioned how ISIL and other terrorist organizations field potential recruits in publicly accessible social networking sites and via encrypted private messaging platforms. Could you detail the issues that law enforcement is facing due to the end of encryption?

Mr. COMEY. Yes, sir. The ISIL challenge illustrates the problem we call Going Dark. That ISIL increasingly uses, when they find someone who I call a live one, that is, someone who they might be able to motivate to engage in acts of violence in the United States,

they move them from Twitter or Twitter direct messaging—Twitter direct messaging is available to us with court process—to a mobile messenger app that is end-to-end encrypted, meaning if we get a court order from a judge and intercept the communication, we can't decipher it, we can't read it. And so those people, their communications become invisible to us even with a court order.

That's the challenge. We actually face that in all kinds of criminal cases as well, but it is very well illustrated by the ISIL challenge. That's what I mean when I talk about that.

Mr. JOHNSON. So, in other words, a foreign based person, a foreign person operating from a foreign location using social network such as Twitter can identify a potential target for radicalization, or someone who's already radicalized but who's reaching out to this foreign based person, and then they can take it to another site where their communications are encrypted, correct?

Mr. COMEY. Correct.

Mr. JOHNSON. And because they're encrypted, then law enforcement, whether or not it has a warrant or not, cannot discover what they are talking about, even though they know that this foreign-based person is a ISIL member?

Mr. COMEY. That's correct, and we have to have a court order, but the court order would be useless.

Mr. JOHNSON. Yeah. So now the practical impact of that is what?

Mr. COMEY. That we can't know what somebody, who's planning on an act of violence against a police officer or military member or a civilian is up to and when they are going to act, and we're limited to physical surveillance, trying to watch them and figure out what they're going to do or trying to get other ways to get visibility into what they're up to. So it is darkness, or they go dark to us in a way that's really important in those matters.

Mr. JOHNSON. Okay. And you mentioned about traditional crimes, domestic crimes, and how encryption hurts your ability to get at domestic criminal activity. Can you talk about how in a case of hot pursuit or exigent circumstances, this adversely affects our ability to keep Americans safe from domestic crime?

Mr. COMEY. There's lots of different ways in which it impacts. In fact, I believe the going dark problem overwhelmingly affects State and local law enforcement. People talk about it like it's an intelligence question, but it's actually almost entirely a law enforcement question because—I mean, to give you an example that a lot of DAs talk about. If they recover a cell phone, right, at a scene where someone has been murdered or been kidnapped, they cannot open the device, even with a court order, to figure out who was that person communicating with before they disappeared? That's the most basic example.

We also are increasingly encountering it where drug gangs or carjacking gangs are communicating using apps, text apps that are encrypted end to end and with a court order we can't read. So it's becoming increasingly—the logic of it is, it will affect all of our work at some point. Hundreds and hundreds of cases will eventually be affected by it because it is all of our lives are becoming part of the digital world. And when the digital world is covered by strong encryption, judges will not be able to order access in serious criminal cases or in national security cases. That's the future we're

coming towards, and my view is maybe that's where we want to be, but we ought to talk about it as we're going to that place.

Mr. JOHNSON. Well, thank you for your responses to my questions.

And I'll yield back.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Utah, Mr. Chaffetz, for 5 minutes.

Mr. CHAFFETZ. I thank the Chairman, and Director, thank you for being here.

The FBI has had to change through the course of time since my grandfather, who was a career FBI agent, served. I have great admiration for the agency and what you in particular are doing.

I want to go back to cyber, we've talked a lot about cyber. Can you articulate the size, scope, and investment that you in both personnel, dollars to address the cyber threat that's going to continue in perpetuity?

Mr. COMEY. Thank you, Congressman.

I probably can't give you exact numbers sitting here, but we have a cyber division headquarters that does nothing but cyber-related work and then cyber task forces in every single FBI field office, cyber squads, but that doesn't quite capture it because all of the threats we're responsible for come at us through the Internet now, whether it's kids being protected or terrorists coming after us, and so everybody actually has to be, in a way, a cyber analyst or a cyber agent. So I could give you specifics on how many hundreds, thousands of people are assigned to do cyber work, but it's actually even broader than that.

Mr. CHAFFETZ. What is it that you can't do? That is, is there another department or agency that's doing something that the FBI couldn't do?

Mr. COMEY. In the cyber realm?

Mr. CHAFFETZ. Yeah.

Mr. COMEY. That's a good question.

Mr. CHAFFETZ. Well, thank you.

Mr. COMEY. Yeah, I can't think of it sitting here. Our responsibilities are obviously confined to the United States, and so we work with our partners, NSA, in particular, in trying to fight the cyber threat that's coming from overseas. The bureau doesn't have the ability to reach out in that way, and so that's something we can't——

Mr. CHAFFETZ. Let me ask you in the context of the United States Secret Service. I was surprised to learn that the agents that they have, two-thirds of their time is spent on investigations and cyber. And it begs the question to me, why do we have such a small group of people doing that, which the FBI has a much bigger resource, infrastructure, and expertise in doing? And as we look at potentially restructuring the Secret Service and getting more focused on the protective mission, why not combine the two? Or what is it that they do that you don't want to do or that they do that you can't do? I'm trying to get my arms around it.

Mr. COMEY. It was such a good question, I misunderstood it. I'm sorry. One of the things I've been trying to do is drive us closer together with the Secret Service because they have expertise, especially in the financial related intrusions and credit card scams.

They've spent years developing that expertise, and so I don't want to duplicate it, so we're trying to drive ourselves together.

I'd like us to combine our task forces. It doesn't make any sense for them to have an Electronic Crimes Task Force and me to have a Cyber Task Force, there ought to be one. They do great work. I want to make sure we don't duplicate, and I want to do joint training with them. They're doing some great training, so are we. That's one of the things we can't do. We can't do enough for State and local law enforcement to help them deal with digital crimes.

Mr. CHAFFETZ. So in terms of the personnel that you have associated with that, how would that work? Are there other agencies that would also—I mean, Secret Service is but one. Are there other agencies that should be also included in that because we've got a homeland security organization that thinks they should be in charge of all the cyber?

Mr. COMEY. Yeah, I think with respect to the criminal work that we do, there are people at HSI within Department of Homeland Security who are doing cyber-related crime work, and then there's a lot of State and local law enforcement doing it, and they are part of our task forces.

Mr. CHAFFETZ. Can you shed anymore light on the FBI's next-generation cyber initiative? Explain that to me a little bit more.

Mr. COMEY. Without eating up all your time, it's our strategy, my strategy for where we are going to take the FBI in the next 3 to 5 years, and so it involves deploying our people in a different way, getting better training, better equipment, focusing ourselves on the threats that I think the FBI, given its footprint, is best able to address, so it's our sort of whole of FBI approach to cyber over the next 3 to 5 years.

Mr. CHAFFETZ. And so when you have FBI personnel that will focus potentially their entire career just an cyber, correct?

Mr. COMEY. Correct.

Mr. CHAFFETZ. They won't necessarily be bouncing around to different tasks?

Mr. COMEY. Correct.

Mr. CHAFFETZ. All right.

I appreciate the time. I'll yield back.

Mr. FRANKS [presiding]. And I thank the gentleman, and we'll now recognize Mr. Deutch for 5 minutes.

Mr. DEUTCH. Thank you, Mr. Chairman.

Director Comey, thanks so much for being with us today. I represent south Florida, Broward County and Palm Beach County, and we are experiencing an alpha-PVP, or flakka, epidemic. Broward County is the epicenter of the ongoing national flakka crisis. In Broward, the number of cases is spiraling out of control. The Broward County Sheriff's Office has stated that in January 2014, they analyzed a single flakka case. By September 2014, they were analyzing 80 cases. This year, the sheriff's office has reported analyzing approximately 100 cases per month.

Flakka cases are also flooding the county health system. The Broward health system has reported that they're receiving, on average, 12 cases per day. In this past year, it has contributed to the death of 45 people in Broward County.

Flakka use has also started to spread northward into Palm Beach County. In 2014, there were 35 submissions involving flakka to the Palm Beach Sheriff's Office crime lab. In 2015, there have been 42. There have been 10 arrests in Palm Beach County, and flakka is now moving into Tennessee, Kentucky, Ohio, and other the States.

As you're aware, people using flakka experience hallucinations, delirium, violent outbursts, and extreme body temperatures that often cause the users to remove their clothes. Flakka is extremely cheap. It costs $5. And it can be easily purchased online from China. The low cost of the drug and the easy access are very troubling.

Flakka, as is the case with other synthetic drugs, is extremely difficult for law enforcement to prosecute. The primary problem is that the composition of the synthetic drug can't be pinpointed and classified as illegal because the drugs are constantly changing their composition. And as soon as the synthetic drug is listed as illegal, the composition is changed ever so slightly to evade the listing that made the drug more readily available.

In fact, a recent news report in Miami found that flakka is now being made into gummy bears—gummy bears. The only difference between the real ones and flakka gummy bears is that the ones containing flakka are individually wrapped and stickier. Dealers are using them now to hook young people.

So if you could target the efforts that the FBI has taken to crack down on this epidemic of synthetic drugs, flakka, in particular, and speak to the challenge that you face in cracking down on, again, these sorts of cases involving flakka and other synthetic drugs.

Mr. COMEY. Thank you, Congressman. The synthetic, I think the word is cannabinoids, and my friend, Chuck Rosenberg, the leader of the DEA, is probably laughing listening to me mispronounce it, but it is a serious problem that I hear about all over the country.

So DEA obviously has the lead on the Federal level, but we are participating through our drug task forces with DEA in trying to do something about that scourge, which you're exactly right: it's appearing in gas stations or little markets where kids can walk up and buy these things not knowing exactly what they're buying, and it will wreck their life.

Mr. DEUTCH. And the current law permits synthetic drugs to be treated as a controlled substance if they are proven to be chemically and/or pharmacologically similar to schedule I or schedule II controlled substances, but as I pointed out, the nature the drugs keep changing. They change the chemical structure to avoid being listed as a controlled substance, so my question to you is what steps can lawmakers take to help in your efforts, local enforcement efforts, as well, to crack down on this epidemic?

Mr. COMEY. Yeah. I honestly don't know. I from talking to Acting Administrator Rosenberg, that they are keenly focused on that problem, which is every time they schedule one of these things, it comes in from China slightly different, and so it's not scheduled anymore. They are sort of chasing it, playing Whack-A-Mole with a very dangerous substance. I don't know what the answer is, frankly.

Mr. DEUTCH. Well, Director Comey, I would invite representatives of your task force and the DEA to come to south Florida. This is an issue that dominates the headlines. It's an issue that affects young people, and as you point out, the moment that somebody takes this, one of these synthetic drugs, flakka, which is so readily available in Florida and elsewhere, it changes and often ruins their lives. So I'm grateful for your focus on it, and I hope we have the opportunity to do something down in south Florida to really raise the issue so that people in south Florida can know what this focus is and how much we can do about it. Thank you very much.

Mr. COMEY. Thank you, sir.

Mr. FRANKS. I thank the gentleman.

Will now recognize Mr. Marino for 5 minutes.

Mr. MARINO. Thank you, Chairman.

Good afternoon. Good morning. It's good to see you.

Mr. COMEY. Good to see you again, sir.

Mr. MARINO. I, too, am a maniac for the rule of law. As you're aware, most of my adult career was in law enforcement, and I still consider myself a law enforcement guy. My family has been in law enforcement for a long time as well, so I appreciate your comments concerning oversight and the rule of law, and that's needed very much today. I think even more so today, but I do want to emphasize the fact that I've worked with all agencies, State, local, and Federal, and 99.9 percent of our agents out there are topnotch, and I trust them watching my back at any time.

But, with that, you have very effectively answered two questions that I had that I was going to ask you, so as a result, I will yield back the remainder of my time, and best of luck.

Mr. COMEY. Great to see you, Mr. Marino.

Mr. FRANKS. And I thank the gentleman.

I now recognize Ms. Bass for 5 minutes.

Ms. BASS. Thank you, Mr. Chair.

And thank you, Director, for coming and testifying today.

I'd like to talk about the recent operation cross traffic, FBI's nationwide effort to crack down on child sex trafficking. The FBI's October 13 release about the operation states: "Operation Cross Country, a nationwide law enforcement action that focused on underage victims of prostitution has concluded with the recovery of 149 sexually exploited children and the arrest of more than 150 pimps and other individuals."

And, first of all, I'd like to commend the agency for correctly referring to the children as sexually exploited children versus prostitutes because a child who is under the age of consent should never be considered a prostitute.

This release refers to other individuals, and I was wondering who those other individuals were. I have a concern that while it's extremely appropriate to focus on the pimps, it's also, in my opinion, very much appropriate to focus on the child molesters who some people would call Johns, but I would like to know if that's who you were referring to, and what is the focus on the child molesters?

Mr. COMEY. Yes, Congresswoman, that is what I understand was meant by that. There were more than 100 so-called Johns arrested

as part of Operation Cross Country along with the pimps and the children being exploited.

Ms. BASS. Thank you. The release also says that the children were recovered, and I wondered what does that mean. So what has happened or will happen with the children?

Mr. COMEY. As part of Operation Cross Country, the folks I call the angels of the FBI, which are our victim specialists, are deeply involved in the operation to make sure that those kids get either reunited with their families, or so many of them come from foster care.

Ms. BASS. Right.

Mr. COMEY. If they get in a new placement, a healthier placement, a lot of them need medical attention right away. And that's what was meant by that, to get that child to a place where they are cared for either by the biological family or a placement in a foster family.

Ms. BASS. And in addition to medical attention, they certainly need a tremendous amount of therapy. I think it's important, you know, in the future, I would appreciate it if you would lift up—where you were saying that the other individuals were referring to the child molesters, I think it's really important that we focus, we call it correctly and that we focus on that.

In addition, I would also like to know if the FBI tracks the number of children that are in foster care. We know that a large percentage of these kids are in foster care, but there's not a lot of documentation. Do you have documentation that could give us some numbers?

Mr. COMEY. I think we do. I think our intelligence analysts, who support an effort like this, have done some good work on that front. I'm a foster parent, so they know it's a passion of mine.

Ms. BASS. Oh, I didn't know that.

Mr. COMEY. And so I think we could equip you with at least some of our thinking on it as we do this work.

Ms. BASS. Great. Well, I would like to follow up with your office and get that data.

I'd also like to commend you for your Innocence Lost Task Force, and I'd like to know if there's more that we can be doing to assist your efforts in Innocence Lost. I work with them in the Los Angeles area, and you know, you have been in the leadership of bringing different sectors of law enforcement together to understand this problem and address it.

Mr. COMEY. Well, I appreciate your interest in it, and I will ask my staff to think about ways in which we might get more help. We appreciate the offer.

Ms. BASS. Okay. Thank you.

And I yield back my time.

Mr. FRANKS. And I thank the gentlewoman.

We now recognize Mr. Labrador for 5 minutes.

Mr. LABRADOR. Thank you, Mr. Chair.

Mr. Director, it's great to have you here. I have heard from many of my constituents about the refugee program and its impact on Idaho. As refugee admissions are increasing, there is growing concern that bad actors are not being caught in the vetting process

and are gaining admission alongside bona fide refugees living in fear.

I'm actually an advocate of refugee programs. I think it's a good thing to have refugee programs, but there's a lot misconceptions out there and a lot of real fear about the people that are coming into the United States. This Congress has an obligation to address those concerns and ensure that the process is working correctly and protecting our national security.

Numerous times over the past year, including yesterday, both the FBI's Assistant Director for the Counterterrorism Division Michael Steinbach and yourself have testified about the flaws and limitations in the vetting of Syrian refugees.

On October 8, you testified that you were concerned about certain gaps in the data available to the FBI, and yesterday you testified that the FBI can only query what has been previously collected, which is obvious.

I know that you have addressed this issue before and you've addressed it, I think, once here today, but can you please explain to this Committee the security gaps that exist for purposes of conducting full and effective background checks on foreign nationals who claim to have fled the conflict zone of Syria and who are seeking to be resettled as refugees in the United States?

Mr. COMEY. Certainly. Thank you, Mr. Labrador. We learned some good lessons from less than excellent screening of Iraqi refugees 8 years ago or so, and in fact, we learned that some folks we had let in were serious actors that we had to lock up after we figured out who they were. And so we have gotten much better, as an intelligence community, at joining our efforts and checking our databases in a way that gives us high confidence. If we have a record on somebody, it will surface. That's the good news.

The bad news is, as we talked about earlier, with Iraqi refugees, we had an opportunity for many more encounters between folks in Iraq and our soldiers, for example, so we had a lot more data. We had fingerprints, iris scans, we had forensics of different kinds. The challenge we face with Syria is that we don't have that rich a set of data, so even though we've gotten better at querying what we have, we certainly will have less overall.

And so as I said to a question earlier, someone only alerts as a result of our searches if we have some record on them. That's the challenge we face with Syria.

Mr. LABRADOR. So is it accurate to state that the lack of intelligence available on the ground in Syria is rendering our traditional database biographic and biometric checks obsolete?

Mr. COMEY. I wouldn't agree obsolete, but I would say we have a less robust data set dramatically than we had with Iraq, so it will be different.

Mr. LABRADOR. So the FBI has repeatedly contrasted the United States' ability to collect intelligence on the ground in Iraq with its ability to do so in Syria. What can the FBI do to adapt to improve security checks for refugees originating from failed states with no available intelligence?

Mr. COMEY. Well, that's a hard one. What we can do, the FBI, is just make sure that whatever is available figures into our review, but the underlying problem is, how do you generate intel-

ligence in failed states? And that's one I don't have a good answer for.

Mr. LABRADOR. So are you currently working with the intelligence community to try to fix this problem?

Mr. COMEY. Oh, certainly. Everyone in the intelligence community is focused on trying to mitigate this risk by querying well and also finding additional sources of information so we can check against it.

Mr. LABRADOR. Recognizing that ISIS and Syria and that there is a risk that bad actors may attempt to take advantage of this Administration's commitment to bring at least 10,000 Syrian refugees into the United States over the next year, can you estimate the manpower and resources that will need to be diverted from other investigative programs to address this threat?

Mr. COMEY. I'm not able to do that sitting here.

Mr. LABRADOR. How can I ensure my constituents that the people that may come to Idaho are safe, that they are not terrorists, that the people in my community are going to be safe?

Mr. COMEY. Well, on behalf of the FBI, what you can assure them is that we will work day and night to make sure that if there's information available about somebody, we have surfaced it, and we have evaluated it.

Mr. LABRADOR. And I understand that if there is information, but the problem is that we don't have the information on most of these people. Isn't that true?

Mr. COMEY. Yeah, and so I can't sit here and offer anybody an absolute assurance that there is no risk associated with this.

Mr. LABRADOR. Thank you very much.

I yield back my time.

Mr. FRANKS. And I thank the gentleman.

I now recognize Ms. DelBene for 5 minutes.

Ms. DELBENE. Thank you, Mr. Chair.

And thank you, Director Comey, for being here and for your service. I know as Acting AG, you demonstrated a commitment to the Fourth Amendment and protecting Americans' privacy, despite enormous pressure to do otherwise, and you mentioned in your original testimony and in other comments that the rule of law and the Fourth Amendment is the spine of the FBI, and so I appreciate that commitment. I'd like to ask you a few questions about the FBI's use of aircraft.

The FBI deployed aircraft over Ferguson last year in response to requests from local law enforcement. Is that correct?

Mr. COMEY. Yes.

Ms. DELBENE. Does the FBI respond to these types of requests frequently?

Mr. COMEY. Well, thank goodness there aren't the kind of turmoil and pain in communities frequently, but sure. If local law enforcement asks for help in getting a look at a developing situation, we will offer that help. We've done it in Baltimore. We did it in Ferguson, as I recall.

Ms. DELBENE. And what criteria have to be met for the FBI to send aerial resources to assist local law enforcement, or who makes that decision?

Mr. COMEY. It's made at a fairly high level in the FBI. I think at the special agent in charge level, at least that is the commander of the field office, so it has to go up through a variety of checks before it can be approved.

Ms. DELBENE. And what are the criteria that you use to make that decision?

Mr. COMEY. I think it has to be part of an open investigation of ours or part of an open assistance to law enforcement matter. We can get you the particulars of our policy, but as you know, the bureau has a policy for everything, so there's a series of steps that have to be walked through to make sure it's part of either an open case of ours or it's a legitimate open assistance to law enforcement matter.

Ms. DELBENE. Okay. Thank you. I'd appreciate that information.

Your staff also acknowledged that the FBI "routinely uses aviation assets in support of predicated investigations targeting specific individuals, and when requested and appropriate, in support of State and local law enforcement."

Why is it so important to stress this distinction when it appears that it's kind of more generalized type of surveillance?

Mr. COMEY. I'm sorry, the distinction?

Ms. DELBENE. The distinction that you have in the feedback from your staff that you use aviation assets in support of predicated investigations targeting specific individuals when in these cases of local law enforcement, et cetera, it seems to be more generalized type of surveillance.

Mr. COMEY. Oh, I see. Well, I think we're just trying to explain how we use it. We don't fly planes around America looking down trying to figure out if somebody might be doing something wrong. The overwhelming use of our aircraft is a pilot flies as part of an investigation to help us follow a spy, a terrorist, or a criminal, and then with local law enforcement, if there is tremendous turbulence in a community, it's useful to everybody, civilians and law enforcement to have a view of what's going on: Where are the fires in this community? Where are people gathering? Where do people need help? And sometimes the best view of that is above rather than trying to look from a car in the street.

Ms. DELBENE. And do you feel that warrants are necessary when you're targeting specific individuals, especially when you have aircraft equipped with new technologies like high-resolution cameras?

Mr. COMEY. I don't think so. I mean, I meant what I said about the Fourth Amendment. We are not collecting the content of anybody's communication or engaged in anything besides following somebody when we do that investigation, so as I said, we've done it since the Wright brothers with planes, and we do it in cars, and we do it on foot, and the law is pretty clear that you don't need a warrant for that kind of observation.

Ms. DELBENE. But now that there are technology changes—I think even the most recent court case, you know, *Florida v. Riley*, was in 1989—there has been a lot of changes in technology, and so it's not just what you might see with the human eye anymore. So are there other types of technologies, and do you think warrant standards should be in place when you have other types of technologies that might be used on this aircraft?

Mr. COMEY. I suppose if you are putting technology on an FBI aircraft that had Fourth Amendment implications, that is that it was reaching someone's communications or looking within a dwelling or something like that, it would have Fourth Amendment implications. But that's not what we use the aircraft for.

Ms. DELBENE. So what led to the decision to seek court orders when aircraft are equipped with Stingray technology?

Mr. COMEY. Right. We have one aircraft that we can put Stingray technology on it, that is cell-site simulators, and I suppose we can mount it on others if we had a court order to do it. But we have decided as a matter of policy—now the whole Department of Justice does this—that if we're going to be operating a cell-site simulator, it has Fourth Amendment implications, so we will get a warrant for that. So whether that's on the ground or in an airplane, we treat it the same way.

Ms. DELBENE. You said you decided. Do you feel like that you're required by law to do that?

Mr. COMEY. I think we made that move before there was even a divide among opinions in the court. Some courts have said you need it for that, some not. We went nationwide with a requirement for warrants. There has been no national decision on that, no Supreme Court-level decision on that, but we just think, given that some courts are requiring it, we do it across the country.

Ms. DELBENE. Thank you. My time has expired.

Mr. FRANKS. I thank the gentlewoman and now recognize Mr. Buck for 5 minutes.

Mr. BUCK. Good morning, Director Comey.

Mr. COMEY. Good morning.

Mr. BUCK. I wanted to ask you, do you remember Mr. Cohen's questions about renaming the FBI headquarters building earlier?

Mr. COMEY. Yes.

Mr. BUCK. And I appreciate your response that we have to look at things through the lens of history. I wanted to ask you about a few other historical figures and see if there were any other FBI buildings named after some of these folks.

Former Democrat Senator Robert Byrd of West Virginia was a member of the KKK. He was a recruiter for the KKK, and he held leadership positions with the KKK. The State Capitol in Charleston, West Virginia, is named after Senator Byrd. The United States Courthouse and Federal Building in Beckley, West Virginia, is named after Senator Byrd. The United States Courthouse and Federal Building in Charleston, West Virginia, is named after Senator Byrd. And the Federal Correctional Institution in Hazelton, West Virginia, is named after Senator Byrd.

My question is, do you know of any FBI buildings named after Senator Byrd?

Mr. COMEY. I don't know. And I don't know whether we have folks sitting in the courthouse. I just don't know sitting here.

Mr. BUCK. Okay. Former Democrat President Woodrow Wilson resegregated the entire government, including the Armed Forces, held a showing of the movie "Birth of a Nation" at the White House, and went so far as to praise it in spite of calls by the NAACP to ban it. "Birth of a Nation" was subsequently used as a recruiting tool for the Ku Klux Klan. Likewise, there are a number

of buildings around this country named after President Wilson. In fact, there is a bridge leading in and out of Washington, D.C., named after President Wilson.

Do you know of any buildings that the FBI occupies or predominantly owns that are named after President Wilson?

Mr. COMEY. I don't.

Mr. BUCK. Former President Lyndon Baines Johnson was fond of using the "N" word, used it in the White House, used it while he was Senate majority leader, and used it in many other public settings. Many Federal buildings are named after him.

Are there any FBI buildings named after President Johnson.

Mr. COMEY. I don't know.

Mr. BUCK. And lastly, President Truman wrote to his soon-to-be wife the following words: "I think one man is just as good as another so long as he is not a 'N' word or a Chinaman." Again, many buildings named after President Truman.

I'm just wondering, any FBI buildings named after President Truman?

Mr. COMEY. I don't know, sir.

Mr. BUCK. And last after last, Democrat Senator Richard Russell was also a member of the Ku Klux Klan, and there is a Senate building named after Senator Russell. I assume there are, at least to your knowledge, no FBI buildings named after Senator Russell?

Mr. COMEY. I don't know. I don't think so, but I don't know.

Mr. BUCK. And my last statement I guess would be that perhaps Congress should clean up its own act in naming buildings before it asks the FBI to, without the lens of history, try to rename buildings.

I yield back my time.

Mr. FRANKS. And I thank the gentleman and now recognize Mr. Cicilline for 5 minutes.

Mr. CICILLINE. Thank you, Mr. Chairman.

Thank you, Director Comey, for your service and for coming before the Committee today and for sharing your valuable insights. And thank you also to the extraordinary men and women who serve the Bureau and help keep our country safe, and I think our entire Nation owes them a debt of gratitude.

Many us expressed our sincere concern and condolences following the recent mass shooting in Roseburg, Oregon, where nine innocent men and women lost their lives. Many of us have shared the same sentiments following tragically similar events in Lafayette or Newtown and Blacksburg.

But as more Americans lose their lives to senseless gun violence, this Congress has failed to act. And, Director Comey, with this in mind, I'd like to draw on your experience to help us find solutions to this growing epidemic and to help us find the guts to take necessary action.

And so first I want to just draw your attention to the shooting which occurred at the Emanuel African Methodist Episcopal Church in Charleston, South Carolina. Following the shooting, you ordered the FBI to conduct an internal review of policies and procedures surrounding background checks for weapons purchases. So my first question is, did that review occur, and what were the findings of that review?

Mr. COMEY. Thank you, Congressman. The review did occur. I asked my folks to do a 30-day examination, and two things came out of that. First, it confirmed the facts as I understood them. There were no new facts with respect to Dylann Roof's purchase in particular that changed. And then it highlighted two potential areas for improvement, one internal to the FBI, one external.

Internal, it highlighted for us that maybe we can surge resources and technology to try and reduce the number of gun sales that are held in the delayed pending status longer than 3 days, and so that work is underway. And then secondly, to get better and more timely records from State and local law enforcement about the disposition of people's arrests so that our examiners have good records to make a judgment on. And those conversations are ongoing.

Mr. CICILLINE. So those are actually the two areas I'd like to discuss. As you well know, the current law requires that if a requested purchase of a firearm is made, a background check is initiated, the FBI has 3 days to respond. If no response is provided, then the gun dealer is able to sell the weapon. My understanding is the FBI continues the review anyway, even in it's beyond the 3 days. That information is then conveyed to the gun dealer, and if that person is disqualified from buying a gun, what does the FBI do? So you now know a sale has occurred—or do you know a sale has occurred—and do you take action?

Mr. COMEY. Yes. If after the 3-day window the gun is transferred and then the examiners discover disqualifying information, my recollection is—and if I'm wrong, we'll fix this—a notice is sent both to local law enforcement in that jurisdiction and to the Bureau of Alcohol, Tobacco and Firearms so that they can retrieve the firearm from the prohibited person.

Mr. CICILLINE. So I would like to work with you on that because I'm not sure that that is actually the practice. I think that notice may go to ATF, but I don't believe it goes to the gun dealer or to local law enforcement. And I think that's a way that we can try to keep guns out of the hands of people who don't have them, and I would very much like to work with you on that.

The second issue is how do we incentivize, require, encourage local law enforcement to actually use the NICS system? Because that background check system is only as good as the information that's in it. Have you done an analysis of what States participate, where the deficiencies are, or things we could do or that Congress can do to help ensure that more States are providing that disqualifying information so at the bare minimum we're keeping guns out of the hands of people who shouldn't have them under law?

Mr. COMEY. Yeah. The mass murder in Charleston was an event that I think caused a lot of folks in local law enforcement, State law enforcement, to focus on this question. And as I said, there's a whole lot of conversation going on, and we are pushing out training to State and local law enforcement to explain to them what we need and why we need it in a timely fashion.

I don't have as I sit here suggestions for how Congress might help us incentivize that cooperation. I think they're good people, and when they see the pain of a situation like Dylann Roof's, they want to be better. But I will get back to you if I have ideas for how Congress can help.

Mr. CICILLINE. Because, as you well know, Director, we can't require participation with the NICS system as a result of a Supreme Court decision, but we ought to be able to do things to create serious incentives or maybe penalties for States that fail to furnish that information, because as a result of that information not being in the NICS system, people are walking into gun stores and buying guns who would be otherwise disqualified if that information were known.

So I look forward to working with you on that. I think it should be an urgent national priority, and I thank you for the work that you're doing.

I yield back.

Mr. FRANKS. I now recognize the gentleman from Georgia, Mr. Collins, for 5 minutes.

Mr. COLLINS. Thank you, Mr. Chairman.

Thank you, Director, for being here, and I appreciate it. My father, as well as some of the others, my father was a Georgia State trooper for all his life, 30-plus years. So I appreciate your commitment to law enforcement and being a part.

I do have some quick questions that I wanted to go back on. One has to do with an advisory that was put on October 8 for dealing with credit cards and the chip issue here that was for consumer fraud, stated that new credit cards equipped with the microchip security technology were still vulnerable to identity theft and that the use of PIN authentication in addition to a chip would be a more secure way that consumers' transactions would be more simple, signature verification. However, within 24 hours that advisory was taken down and a few days later issued an advisory that no longer included the PINs.

Now, it's my understanding Canada, Australia, many other countries have encouraged the PIN authorization because it, frankly, has a lower fraud rate.

My question would be is, in light of that, does the FBI consider PIN as a more secure form of authentication over signature verification?

Mr. COMEY. I think the experts at the FBI would say that PIN-and-chip is more secure than PIN-and-signature. And the confusion there was our folks put out that public service announcement, and it was a miss on our part, without focusing on the fact that most merchants in the United States don't have the capability to accommodate the PIN-and-chip. And so the worry was that's going to cause a whole lot of confusion when people start saying where's the PIN-and-chip when our equipment is set up in this country for PIN-and-signature.

Mr. COLLINS. Okay. Well, let's talk about that a second, because many of the places that I go to you either swipe—they're older cards, you just swipe, like on a gas station, or you go into—I used to own a store. We had a swipe machine. Many of them now have the—and many of those even with a swipe machine have a number for debit cards which is already there for the PIN. I know now, I've just gotten broken into using the chip because my new cards have chips, so I slide them in. I'm still learning how to do this. But the keypad is right there above it.

I'm not sure I follow your answer there that the technology is not available. If the keypad is right there to input a number, why is the technology not available?

Mr. COMEY. I don't know. And I'm not the world's smartest person on this, but what I've been told by my folks is it is available in some places, but it's not widely available in the United States. And if I'm wrong about that, we'll correct that.

Mr. COLLINS. I'm just going on my own personal. And, look, my, Doug Collins, me going into the store and putting my card in. I've rarely found one that is just pure swipe with no keypad, I think. And I was just concerned, and if that's not right and if you want to go back and look into that.

I think the concern came among many that maybe there is also an issue because as a business owner myself, I paid different fees depending on how I did it, like if a consumer used a credit card versus a debit card. And I'm just wondering, could that have been an issue, because using the PIN typically is a different fee? Was that possibly taken into account as the reason for the removal of this and changed to say, well, it's not as worrisome as we first thought?

Mr. COMEY. No. I think that could be the reason that, if I'm right, that the equipment is not widely available in the United States, that people don't have an economic incentive to change. But that was not a factor in why we withdrew the public service announcement. My understanding is we withdrew it because our worry was we're going to confuse a whole lot of people who are going to roll into places saying where is the chip-and-PIN and it isn't widely available. That's, as I understand it, that was the concern.

Mr. COLLINS. Well, it is. And it's like everything, there was a lot of times before debit card. I think the concern here is, as we deal in information security and everything else, is you're always trying to move toward the more secure atmosphere. That's my only concern. And by moving back on that, it seemed like, at least in my opinion, that we're saying, okay, there is a better way, but we're not going to encourage that, we're just going to let the, you know, let the status quo sort of stand. So it was just a question.

I do have a question. We hit ECPA earlier and the e-mail privacy, which I have a great interest in. One was said is basically the 180-day distinction in current law is something that we have talked about. You said that you use a warrant in all cases. It doesn't matter. Would you say that 30, you know, 30—and there's been statements 30 prosecutors, former judges, all say that requiring law enforcement to obtain a warrant from a court does not prevent law enforcement from doing its job. Would you agree with that, especially in light of this issue?

Mr. COMEY. I think by and large that's true. I think it poses unique challenges for our colleagues at the SEC, for example, investigating corporate fraud, but I think by and large for law enforcement judges are available, and if we have the evidence, we can make the showing. So I think at a general level, sure.

Mr. COLLINS. But in a general level, and also from your high standards as the FBI, I've always considered high standards, even the SEC, some of these agencies, that a warrant, whether they use

it or not, they like it or not, I think from a law enforcement standpoint, from a concern standpoint, from a warrant standpoint, this is something that they could use that they could go through normal means in the investigation. I think that's the concern that many of us have.

There is time for other questions, the hacking issues with OPM and China. Just a quick question, from the FBI's perspective, have we actually traced that and say, yes, for a fact, that we confirm that Chinese hackers stole this data from the OPM?

Mr. COMEY. I have with high confidence an understanding of who did it. I'm not in a position to say it in an open forum.

Mr. COLLINS. Okay. And maybe we can get back on a different forum and discuss that, because like I said, that is a concern. We can't reward bad behavior, and I'm concerned that's what we're doing.

With that, Mr. Chairman, I yield back.

Mr. FRANKS. And I thank the gentlemen and now recognize Mr. Jeffries for 5 minutes.

Mr. JEFFRIES. Thank you, Mr. Chair.

And thank you, Director Comey, for your presence here today and of course your great service to this country.

I think you testified earlier today in your belief as to the efficacy of mandatory minimums. Is that correct?

Mr. COMEY. Yes. I think I said they were a useful tool in my career as a prosecutor, especially in eliciting cooperation.

Mr. JEFFRIES. And can you just elaborate as to whether you still believe that mandatory minimums in light of the explosion of the United States prison population, particularly relative to every other developed country in the world, is still a relevant law enforcement tool?

Mr. COMEY. I think it is. Again, I'm not in a position by expertise, and I shouldn't in my job offer a view on whether it ought to be 10 years or 5 years, but I think the certainty of punishment is a useful tool in fighting crime. And in the absence of mandatory guidelines, that often comes in the form of a mandatory minimum. But that's about as far as I have the expertise and the position to go.

Mr. JEFFRIES. And is your view anchored in the fact that many prosecutors have articulated the position that in the absence of mandatory minimums they don't have the same club by which to solicit cooperation and perhaps obtain plea bargains? Would that be part of your view here?

Mr. COMEY. Yes. In my experience and comparing my experience with the State system, which did, again, in my experience as a prosecutor, did not have the tools to elicit cooperation that we did. But, again, that's not a view on whether it ought to be this or it ought to be that. I don't have the expertise, or I'm not in a position to offer a view on that. But some certainty of punishment absent cooperation is very, very valuable in eliciting cooperation.

Mr. JEFFRIES. Now, there have been studies that have shown that in crimes that actually don't have mandatory minimums, the conviction rates at the Federal level are actually higher than the conviction rates of those where mandatory minimums do exist. And so I think that's part of the reason why an ideologically diverse

group of individuals on both the left and the right, including the Heritage Foundation, which I believe said there's no evidence that mandatory minimums reduce crime, have questioned their continued need, at least in its current form.

Now, can you comment on sort of the explosion of the United States prison population. When the war on drugs began in the early 1970's, we had less than 350,000 people who were incarcerated in America. Currently that number is in excess of 2.3 million.

As you know, we've got 5 percent of the world's population; 25 percent of the incarcerated individuals in the world are here in the United States of America. Many of us believe it creates a competitive disadvantage for us going forward in addition to the damage that it does to the social fabric of many communities.

Could you comment as to the mass incarceration phenomenon that exists in America and what, if anything, you think should be done about it from a public safety standpoint?

Mr. COMEY. Sure. I struggle with the word mass incarceration because it conveys a sense that people were locked up en masse when every case in some respects is a tragedy, in my view, but every one was individual, everyone had a lawyer, everyone had a judge, everyone had to be proven guilty.

There is no doubt a whole lot of people are locked up, and that is a big problem for our country in one respect. But here's the fact: In 2014, America was far safer than it was when I was born in 1960. And I think a big part of that change, as a result of which a whole lot of people are alive today who wouldn't be, is due to law enforcement.

And so I'm of a view that, yes, we can reform our criminal justice system. It can be better in a lot of ways. But we ought to reform it with an eye toward where we used to be and how we got from there to here, because I would not want to give back to our children and our grandchildren the America that we lived in, in the 1970's, 1980's, and 1990's. That's the reason I want us to be thoughtful about it.

But I believe we can be better in a whole lot of ways that we probably don't have time to talk about.

Mr. JEFFRIES. I certainly think it's important for us to be thoughtful. I grew up in New York City in the 1980's in the midst of the crack cocaine epidemic, 2,000-plus homicides in the city of New York alone. We're down under 350. And obviously no one wants to return to that.

A Pew study, though, however, I believe concluded that in all 17 States that have cut their incarceration rates, they've experienced a decline in crime over the past decade. And so it seems to me that there's room empirically, based on the data, for a real discussion as to how to get the balance correct. I gather you share that view.

And I just appreciate your willingness to continue in a dialogue for us to get the benefit of your views as we move forward toward criminal justice reform.

Mr. COMEY. Thank you. Happy to. Thank you.

Mr. JEFFRIES. Thank you.

I yield back.

Mr. FRANKS. I thank the gentleman, and I now recognize——

Mr. COHEN. Mr. Chairman, can I be recognized for a point of personal privilege?

Mr. FRANKS. The gentleman is recognized, without objection.

Mr. COHEN. Thank you, Mr. Chair.

I'm a student of history, and when I make a mistake I want to correct it. And I was wrong in saying that Senator Vandenberg's son had committed suicide. It was a Senator Hayes, and his son was arrested in Lafayette Park for being gay. But that was McCarthy who was after him. So it was right church, wrong pew, but I wanted to correct the record.

Thank you, sir.

Mr. FRANKS. I thank the gentleman.

I now recognize Mr. DeSantis for 5 minutes.

Mr. DESANTIS. Good afternoon, Director Comey.

I've noticed—I'm a former prosecutor—companies have begun notifying customers when law enforcement requests data through a subpoena or warrant unless there is a court ordered nondisclosure requirement. And I think particularly for, like, child pornography investigations this may be an issue. Do you think that that that's something that could hamper investigations?

Mr. COMEY. I do. It's something I've been hearing more and more about over my 2 years in this job from prosecutors who are worried about it.

Mr. DESANTIS. Okay. I think we're going to address that, so I'm glad to hear you say that.

The President has a plan to bring over a lot of people from the civil war in Syria, tens of thousands, perhaps as many as 100,000. Can we vet them? And if not, isn't it just a fact that some of those people will be contributing to some of the homegrown terrorism that we have in this country?

Mr. COMEY. Thank you for that question. It's a very important issue that we have talked about a little bit here today. We can vet them. We have gotten better at vetting and learned lessons from the vetting of Iraqi refugees. The challenge we face is we can only vet against data that's been collected with respect to a person, and so the information we had for Iraq was much richer than we'll have for Syria.

Mr. DESANTIS. You can't call up the Damascus police department and get files, correct?

Mr. COMEY. You got it.

Mr. DESANTIS. So there's a problem here potentially, and I know it's going to fall on you then to have to defend the American people once some of these individuals come into the country, and it's just something that I'm concerned with.

There has been talk about reforming sentencing. Is it your view—people will say that drug offenses are nonviolent offenses, but particularly when they get into the Federal system, where these are really significant trafficking offenses typically, is it accurate to say that they're nonviolent or is the drug trade inherently violent, in your judgment?

Mr. COMEY. Well, I guess each case is different. But in my experience anyone who is part of a trafficking organization is part of an organization that has violence all through it, and that whether you're a mill worker or runner or lookout or enforcer, you're part

of something that's suffocating a community. And so I have a hard time characterizing drug organizations in any respect as nonviolent.

Mr. DESANTIS. And in terms of the drop in crime that you alluded to, is part of that simply because there have been stiffer sentences and so habitual criminals are incapacitated and they're off the streets, and therefore our communities are safer?

Mr. COMEY. I believe that was a big part, and I think most experts believe it was a big part of the historic reduction we've seen in crime over my career.

Mr. DESANTIS. With respect to individual offenses, I know there's been discussion about mishandling of classified information, 18 U.S.C. 1924. Just one, does the FBI keep records of all the investigations related to each offense of the criminal code?

Mr. COMEY. I don't know that it's searchable by each offense implicated by an investigation. If a case was charged, then the charged offenses would be reflected in Sentinel—that's our record-keeping—but I don't think every possible charge.

Mr. DESANTIS. So in other words, we know every mishandling of classified information offense, we can look that up, that actually gets brought by the U.S. attorney, but we don't know whether the U.S. attorney declined X number of cases pertaining to that?

Mr. COMEY. I think that's correct, but I also don't know with what clarity our records would reflect, if there were a number of potential violations in a case, whether it would be clear from our case files that it was that.

Mr. DESANTIS. Understood. In terms of handling classified information, there has been just stuff in the press about, well, something needs to be marked classified. And is your understanding of the U.S. Code that if I were to send classified information over an unsecure system, the fact that it was not marked classified, does that mean that I have not committed the offense?

Mr. COMEY. That one, as I did with Chairman Goodlatte, I think I'd prefer not to answer. I'm trying to make sure that, given that we have a matter under investigation now that relates in part to that topic, that I preserve our ability to be seen and to be in reality honest, independent, and competent. And if I start commenting on things that might touch it, I worry that I could jeopardize that.

Mr. DESANTIS. And I think that's an admirable posture, and I think it's one you've shown throughout your career. How does when the President of the United States renders a judgment about a specific case saying that there's no, for example, national security damage if certain information has been disclosed, how does that help the investigation, or does it hurt the investigation?

Mr. COMEY. The FBI is the three things I said earlier, honest, competent, and independent. We follow the facts, only the facts. All we care about are the facts.

Mr. DESANTIS. Well, I have no doubt that that will be how you conduct yourself. I just hope that as you guys do your work, as it moves on to other aspects of our system, that it's based on the merits of the case in every instance and it's not based on political edicts from on high.

So thank you for your time. I appreciate it.

I yield back.

Mr. FRANKS. I thank the gentleman and now recognize Ms. Sheila Jackson Lee for 5 minutes.

Ms. JACKSON LEE. Mr. Chairman, thank you.

And to Director, thank you so very much. You appeared yesterday in front of the Homeland Security Committee and added a great deal of insight. And so I'd like to not pursue a line of questioning but hope to have an opportunity to meet with you on something we began discussing yesterday, which is cybersecurity and the whole role that it plays as really, I'd almost call it another figure, if you will, another entity in this scheme of terrorism.

I am the Ranking Member of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, and with my Ranking Member and Chairman, we are looking to be responsible in addressing, which I believe, issues in the criminal justice system and somewhat overlapping the question of terrorism in this Committee, and certainly in Homeland Security.

Let me just quickly start with a question that I think I introduced in the record yesterday, the No Fly for Foreign Fighters. And we heard testimony that indicated the numbers might be going down, and then I had a number in my notes that there was 250, approximately, Americans who had left to the foreign fight and may be coming back.

The thing that I would say to you is that we must always be prepared. 9/11, the scenario of 9/11 was one that we had never imagined before. We had never imagined an airplane being used as a torpedo. We imagined hijacking. We lived through that. We never imagined. So most time imagination comes with Disney World, but I know that this is a very serious posture.

And so we want to just, hopefully, any extra tool that we can give you with respect to refining and defining the lists that you have to make sure that we have every potential—not every potential—but every foreign fighter. Would that be helpful to you?

Mr. COMEY. Yes, we want to make sure the list is comprehensive. If we could get every foreign fighter on there, that would be great.

Ms. JACKSON LEE. So if we have this legislation, which is to add extra tools to you to ensure that that list is a vetted and a well-updated list, would that be helpful?

Mr. COMEY. I don't know the legislation, but the goal I share is to have a complete, updated, carefully vetted list.

Ms. JACKSON LEE. I appreciate that very much.

Let me move now to guns. I don't want to put words in your mouth, but I imagine—and let me say that I served as a municipal court judge. I would see officers all the time, particularly see them undercover, and with a little smile on my face I'd have to say, "Who are you?" Because, obviously, dealing with some of the matters in local government, they were in some tough places and had to look that way as well.

And I recognize the dangers that our officers face. We had a horrific tragedy in our community in Houston, but we just recently lost an officer again in New York, and we lose officers, as we do with others who are impacted by guns, the 11-year-old who is a child who shot an 8-year-old over a dog, and another youngster, 3 years old, that had a gun, I believe, over this weekend and found it. We never can again imagine the ability of our children.

I ask you the question, why law enforcement is not our biggest champion, not on gun control? I call it gun safety regulation, not on diminishing the Second Amendment, but I call it responsibly handling weapons. Who would want to lose a 4-year-old in a drive-by shooting in New Mexico because someone had a gun?

And so can you answer? We've introduced legislation, and you might want to comment on this in particular, that gives you an extended period of time on this gun check situation, which was one of the horrible situations in the South Carolina nine where you were doing your work or the system was doing its work, but since you weren't heard from, they just allowed this gentleman to get a gun and kill nine people.

But can you answer? We have a number of legislative initiatives, Members of Congress don't want anything to do with taking away your gun, controlling, they want to regulate the safety infrastructure. I've introduced legislation to keep guns away from children.

Mr. Director, in your dealing with law enforcement, the impact that guns have on this, more guns in the United States than people, the impact on the work that you all do, would you answer that for me, please?

And my last thing before you go. There have been a number of church fires. We keep ignoring it. There's a series that just happened. We had another series before. Would you comment on the FBI's work that they're doing?

And if the Chairman would just indulge me, I'd just throw another question there, and I appreciate it. If you take this name down, Robbie Tolan, T-o-l-a-n, who was killed on his front porch—it wasn't a porch, it was a cement driveway of his home. Excuse me. Let me stand corrected. Let me apologize to his mother. He was wounded and still lives with a bullet in his liver.

And the disappointing aspect is that it was an officer who mistook him as an African American male in a stolen car. He was in his mother's car going home to his house in Houston, Texas, in a small city called Bellaire.

And my question is for you to look into what further FBI investigation can go into this case, and I would greatly appreciate it.

If, Mr. Chairman, you would allow him to answer that. I thank you for your indulgence.

Mr. FRANKS. The gentlemen is welcome to answer the question.

Mr. COMEY. Thank you, Ms. Jackson Lee. I will certainly look into it, the last matter.

With respect to church fires, we have not ignored them. Our agents are investigating a number of church fire incidents around the country. We have not found patterns and connections that connect to our civil rights enforcement work, but we are continuing to work on it.

With respect to guns, the people in the FBI care deeply about trying to stop gun violence. What the Bureau does not do is get involved in the public policy legal questions because our job is to enforce the law. We leave it to the Department of Justice to make recommendations as to what the law should be. I think that's a place it makes sense for us to be, but we are passionate about trying to enforce the law against bad guys with guns of all kinds, es-

pecially in our cities where gun violence, especially gang-related gun violence, is increasingly a plague this year.

Ms. JACKSON LEE. Well, proliferation of guns endangers law enforcement across the Nation, does it not?

Mr. FRANKS. The gentlelady's time has expired.

Ms. JACKSON LEE. Well, he was just shaking his head saying yes.

Mr. COMEY. Guns in the hands of criminals endanger all of us, including law enforcement.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Mr. FRANKS. I think all of us would agree with that.

Director Comey, I will now recognize myself for 5 minutes for questions. And I want to thank you for being here. Many people here in the Committee have recognized your unbiased attitude toward enforcing the law as it's written, and I think that speak very highly of you, and I've been very impressed with the cogency and just the clarity of your testimony this morning. I believe that a commitment to independent enforcement of the law is a genuine and sincere conviction on your part.

Director Comey, the Department of Justice has investigated past allegations of possible violations—and I know you've touched on this subject before, so forgive me for sort of rehashing it—possible violations of the Partial-Birth Abortion Ban Act. Indeed, in a letter dated August 4, 2015, responding to this Committee's request for an investigation of possible violations of the Partial-Birth Abortion Ban Act by Planned Parenthood, the Department of Justice stated that, "Since the inception of the Partial-Birth Abortion Act, the Department has investigated allegations of health facilities that are related to possible violations of that law."

Is there any current investigation by the FBI related to Planned Parenthood and the footage that's been released by the Center for Medical Progress at this time that you know of?

Mr. COMEY. As I said in response to your earlier question, I will get back to you and let you know. As I sit here now, I don't have a strong enough grasp of where that stands. I do know letters were sent to the Department of Justice, but I've got to figure out exactly where we are, and I can get back to you.

Mr. FRANKS. Okay. But as far as you know, even apart from the Planned Parenthood videos, do you know if any partial birth abortion ban investigations or enforcement actions have been taken by the FBI?

Mr. COMEY. I don't. I know we have jurisdiction to investigate such things. I believe we have, but I don't know enough to answer that well right here.

Mr. FRANKS. Well, I would appreciate that last part being included in any response you have. Obviously, there's some of us, you know, that think that the rule of law applies to these little ones that have so little ability to protect themselves as well.

Let me shift gears on you. I know there's been several questions asked today about gun violence, and I assure you I agree with your last answer completely that we want to do everything that we can to keep guns out of the hands of criminals and that it's vital for the sake and safety of the public that we do that.

There are those of us that would ask law enforcement do we think that it would be wise to take guns out of the hands of law

enforcement, and almost no one would suggest that, because we believe—I do—that guns in the hands of properly trained FBI agents is a protection to the public.

And from my perspective, that would suggest that it's not the guns, it's whose hands they're in, because it's hard to make a case that if they're on the one hand a protective measure in the hands of police officers, that they're something that can protect and deter and prevent or interdict violence, that they're a good thing and that all of us from almost every spectrum of political consideration would suggest that, then the obvious, reasoned response becomes that it is, indeed, not the guns but whose hands they're in.

So my question to you is, how do we separate the argument so that we are doing everything that we can to prevent those who have lost their Second Amendment rights, who have demonstrated violence toward society or some issue with a mental illness, how do we deal with that while still leaving intact the right to own and bear arms under the Second Amendment by those who follow the law and, indeed, oftentimes protect themselves and sometimes even protect officers of the law?

Mr. COMEY. I think, Congressman, that's a question for others, including Congress. The FBI's role is such that I think it's very important that that not be a conversation debate that we participate in because we don't make policy for the American people. The American people tell us what they think the law should be, how to solve these hard problems, and then we will enforce the law. I think that's critical to us remaining those three things I said, honest, competent, and independent. And so honestly it's just not a question I think the FBI should participate in professionally.

Mr. FRANKS. Well, that's a very reasonable answer. I hope that we can do that. I think it will make your job easier, and it will augment the great work you do for the country.

And with that, I am going to end my question time. Do we have any other—yes, we do. I think that Mr. Bishop is not here. Oh, I'm sorry.

The gentleman, Mr. Bishop, you're recognized for 5 minutes. Flying under the radar there.

Mr. BISHOP. I did. I flew under the radar.

Director, I was here earlier. I apologize for stepping out. I want to begin by thanking you for what you and your entire team does, because what you do on a daily basis is something that most of us don't even know about, we can't comprehend. And you keep us safe, and we're grateful for what you do. And on behalf of my family, my constituents, my State, my Nation, I'm very grateful to you and your entire department. So I wanted to tell you that.

And I admire your testimony today, and thank you for your candor. You've been here forever taking a lot of questions.

I thought maybe I'd asked you about Syrian refugees and what we're seeing. My State of Michigan is a huge hub for those of Middle Eastern descent. There is some concern about the onslaught of refugees into our country. And I apologize if you've answered this question, but I'd like to ask you, what do we know, how do we vet these refugees coming into our country? Is there a way to do it that we can rely upon?

My office does a lot of immigration work. We work with those who are attempting to immigrate legally every day, and we help them any way we can to try and get through, jump through the hoops. It's very strange that we now have groups that are coming in in the way they are that really skip all those steps in between.

So I'm just wondering if you could share with me what your experience is and what you know about the process.

Mr. COMEY. It's a process I describe as good news and bad news. The good news is we have gotten as a country, and the intelligence community in particular, much better at organizing ourselves so that we get a complete picture of what we know about somebody. We learned some lessons from Iraqi refugees 8 years ago or so. And so we have gotten better at querying our holdings. And so if there is a ripple this person has created in our pond, I'm confident that we will see it and be able to evaluate it.

The bad news is we will have less data with respect to folks coming out of Syria than we did with respect to Iraq, because we don't have the U.S. Army presence and all of that that would give us biometrics to query. So the risk is that someone who is a blank slate to us will be vetted by us in a process that's efficient and complete but will show no sign of anything because they've never crossed our radar screen. That's why I describe it as a process that's gotten a lot better but that we can't tell you is risk free.

Mr. BISHOP. And as time goes on, the process that you are going through will be more apparent to the American people. I say that because there are a lot of folks in my State who are very concerned. And, you know, that level of unknown, of not understanding exactly the process, has caused a little panic across the district. And the more that we can hear, the more we understand what the process is.

We remember the Iraqi refugees in the State of Michigan, especially in my area, in southeast Michigan. So I appreciate your ongoing communication on how that's going.

I want to switch gears with you real quick. I've had the pleasure of visiting and working with a number of youth-serving organizations in my district, and I know at least one of those organizations is here today represented. It's important work that they do in the community. And I've spoken to some of them about the importance of keeping their kids safe, and one of the ways to do that is getting background checks. It ensures so many different ways of fostering a safe environment. And it's really an issue I feel very deeply about. I have kids of my own.

Can you talk a little bit about the value of including national FBI fingerprint background checks as a part of the comprehensive screening of staff and volunteers? There are so many that are right there with our children, and we know that the FBI background checks is the gold standard of the process. Can you share a little bit about how we can promote that and encourage that?

Mr. COMEY. Yes. Thank you, Congressman. And I think, if I remember correctly, we have actually been doing a pilot program on that topic at our criminal justice information systems operation, which I do believe is the gold standard. You're right. So anybody who wants to ensure that people in contact with children or in any

other sensitive position have been checked out, the best way to do it is working with us so we can query our holdings.

And as an exciting new feature that's coming on now as part of our Next Generation Identification, we're building in something called Rap Back, which means if you query somebody as a daycare provider, if they are ever again arrested, you will get notified, because that's been a hole in the system. People are clean when they first go in. Then they get in trouble 5 years down the road. You never tell the daycare about this. So Rap Back will make a big difference and make the gold standard platinum in a way. So I very much agree with your sentiment on that topic.

Mr. BISHOP. Did you say Rap Back?

Mr. COMEY. Rap Back, R-a-p B-a-c-k. So if someone develops a rap sheet, we get back.

Mr. BISHOP. Got you. All right. That's the connotation. Okay.

Sir, thank you very much for your time. I appreciate all your testimony today.

With that, I yield back.

Mr. FRANKS. I thank the gentleman, and I apologize for missing him the first time.

And I now recognize Mr. Ratcliffe for 5 minutes.

Mr. RATCLIFFE. Thank you, Mr. Chairman.

Director Comey, thanks for being here. It's good to see you a second day in a row.

Mr. COMEY. Yes, sir.

Mr. RATCLIFFE. I want to ask you a couple cybersecurity issues. Before I do that, I did want to follow up from a question I asked you at the Homeland Security Committee yesterday. We had a brief exchange about the President's decision to take in 10,000 Syrian refugees over the next year. And as we talked about, that's a 500 or 600 percent increase over prior years.

And I had indicated to you that, humanitarian concerns aside, I was troubled with respect to the national security aspects of it, as you're hearing from many of my colleagues here, particularly because ISIS has said that it would use or would try to use the refugee process to get into the United States. And further to that point, as you've testified, our own databases don't have information on some of these individuals, so there are gaps of intelligence there.

So we had a discussion about that figure of 10,000 yesterday. I guess if you had been the sole decider on that issue, what figure would you have recommended to the President?

Mr. COMEY. I don't know. And I'm pleased to say it's not my job to recommend that to the President. I just don't know.

Mr. RATCLIFFE. Well, I understand that. I know the FBI is not a policymaking body with respect to that issue. But as you recall, we had a discussion. I asked Secretary Johnson the same thing, and he assured me that there was an interagency process.

But I guess what I'm trying to get at was, is this a figure that the Administration presented to you and said, you know, meet the security obligations that come with this, or was this part of a process where there was actually input from folks like you that should be providing input on what that number would be?

Mr. COMEY. I think there was plenty of input from the FBI and other parts of the intelligence community on sort of how we

thought about the good news and the bad news. I don't know and don't recall and don't know if I could say even if I did recall how a number came up. It wouldn't have come from the FBI. But I just don't know.

Mr. RATCLIFFE. Okay. Well, you understand the concern that we would hope that these decisions were driven by intelligence rather than political reasons or pressure from our European allies or other folks around the world. And so that's why I asked the question.

But turning to cybersecurity, and I Chair the Subcommittee on Cyber at Homeland, and in your written testimony you said—I want to make sure I get this right—"An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated." And I want that to sink in for everyone because it's such an important point for us to consider in our oversight of the FBI. I think it really speaks to the gravity of the issue here that you're seeing a cyber element to almost every national security threat and crime problem.

So aside from the encryption issue, which I've had the opportunity to hear you talk about in the past, what are the major challenges that you face in detecting and prosecuting cybercrime right now at the FBI?

Mr. COMEY. Thank you for that question and thank you for your interest in that issue and your leadership there.

Two big issues are getting the right folks and the right equipment, in reverse order. The bad guys have very sophisticated equipment, and so if we're going to be good at responding to all the threats we're responsible for, we got to make sure we have world class systems.

And then we got to have great people to operate them, and that's a challenge when we're facing a cybersecurity industry that will pay young folks a lot of dough to go work in the private sector. We compete on mission. I tell these people you're not going to make much of a living, you're going to make a great life. I hope that convinces their families as well, but those are the two big focuses for us.

Mr. RATCLIFFE. Terrific. Thank you, Director.

So the issue of insider threats has been described by at least some as the greatest threat to businesses that operate in cyberspace. And of course we all saw the scale of that threat with respect to Edward Snowden. I know that the Department of Justice has asked Congress for clarity on the law in this area for assistance in prosecuting insiders who access sensitive data that they're not authorized to, and I want to give you an opportunity to elaborate on that from your perspective.

Mr. COMEY. It's an important part of the threat. That's absolutely true. I don't know what the Department's questions and concerns are about their legislative authorities on that front, so I don't think I can offer anything useful there.

Mr. RATCLIFFE. Okay. Well, good.

My time has expired, but like everyone else, I want to express my thanks. Of course I had the opportunity to work for you, both when you were the Acting Attorney General and as the Deputy Attorney General, and because of that I have great confidence in you. And I am grateful for your continued service and am comforted by

the fact that you're in the Director's chair and that you're the person making such important decisions about our Nation's security. So thank you.

And with that, Mr. Chairman, I yield back.

Mr. COMEY. Thank you.

Mr. FRANKS. Well, I would take a moment to echo those comments. With 7-year-old children, we're grateful that people like you are on the job.

This would conclude today's hearing. Thanks to our distinguished witness for attending. Thank the audience here. Grateful to all of you for being here.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witness or additional materials for the record.

And with that, thank you again, Director Comey.

This hearing is adjourned.

[Whereupon, at 1:01 p.m., the Committee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Questions for the Record submitted to the Honorable James B. Comey, Director, Federal Bureau of Investigation*

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-3951

November 19, 2015

The Honorable James B. Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Comey,

The Committee on the Judiciary held a hearing on oversight of the Federal Bureau of Investigation on October 22, 2015 in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Committee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers by January 21, 2016 to Kelsey Williams at kelsey.williams@mail.house.gov or 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact or at 202-225-3951.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

Enclosure

*__Note:__ The Committee did not receive a response to these questions at the time this hearing record was finalized and submitted for printing on March 21, 2016.

Questions for the record from Chairman Bob Goodlatte (VA-06):

FBI Management and Budget Issues

1. With broad responsibilities on the shoulders on the FBI and finite resources, what is your strategy to balance those responsibilities, including counterterrorism, counterintelligence, cyber, and criminal investigations?

2. I understand that there exists a backlog of background checks at the FBI for both incoming and current FBI employees. I am concerned that the Bureau's business is vulnerable to various disruptions if applicants and employees are not cleared. What is being done to ensure that the backlog is reduced?

3. What is the FBI doing to ensure that middle management receives necessary management training and what are the ramifications for FBI managers who fail to receive positive feedback from employees whom they supervise?

4. Do you feel that the FBI is in need of additional resources? More agents? More analysts? More attorneys? Other human capital?

5. Every government agency succumbs to wasteful spending at some point. In your role as Director, describe some ways you are ensuring that the FBI is not wasting taxpayer dollars?

6. Through climate surveys, are you able to address issues of morale in your various divisions to ensure that they are operating effectively? Assuming mandatory participation in climate surveys, have any particular climate surveys and results given you concern? If so, what is being done in those divisions to improve morale and effectiveness?

7. What program areas or offices of the Bureau could be cut in order to shift resources to more pressing national security or criminal functions?

U.S. Critical Infrastructure

1. As more companies move to the "cloud," is the FBI concerned that various companies will no longer have points of presence in the U.S.?

Violent Crime

1. The country is experiencing too many tragedies from mass shooters and these incidents repeatedly raise questions about how individuals with mental illnesses and drug addiction are able to purchase guns to carry out their violence. Congress has tried to motivate

states to provide relevant mental health records on individuals to the National Instant Criminal Background Check System (NICS), the database containing criminal histories used to conduct background checks on gun purchasers. GAO reported that states were making slow progress in providing these records. Additionally, Dylan Roof's admission of a drug crime should have triggered an automatic rejection of his gun purchase if the information had been properly recorded in criminal-record and background-check databases. However, the data was not properly entered in databases.

a. Has the FBI learned any best practices from the Roof mix up of information? If so, are those being communicated to our state partners who are responsible for uploading a bulk of the prohibitive information?

b. Is the FBI seeing improvements and increased numbers of records?

c. Does the FBI have any suggestions for better achieving these goals?

2. Over the past 20 years, the United States has witnessed a marked reduction in violent crime across the nation. However, in recent years, violent crime has dramatically increased in some urban areas like Chicago, Baltimore, and right here in Washington, D.C.

a. To what do you attribute the reduction nationwide? To what do you attribute the recent increase in our urban areas?

b. What is the FBI doing to help alleviate the violent crime increases in our cities?

Hair Review Task Force

1. From a Washington Post Article: "It is critical that the Bureau identify and address the systemic factors that allowed this far-reaching problem to occur and continue for more than a decade," the lawmakers wrote FBI Director James B. Comey on March 27, as findings were being finalized.

a. In the last year, the FBI Laboratory has come under considerable scrutiny in regards to its analysis and testimony of hair cases. Can you give us an update on where the Bureau stands in regards to identifying and addressing systemic factors that allowed this to occur?

b. The FBI's website reported, "The United States Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Innocence Project, and the National Association of Criminal Defense Lawyers (NACDL) reported today that the FBI

has concluded that the examiners' testimony in at least 90 percent of trial transcripts the Bureau analyzed as part of its Microscopic Hair Comparison Analysis Review contained erroneous statements." Could you describe the standard of review that was used in coming to this conclusion? How was this standard of review determined to be the proper standard for reviewing the examiners' testimonies?

c. Were the statements made by examiners at the time of their testimony the accepted science at the time, or do the so-called "erroneous" statements diverge from commonly accepted science both then and now? Please provide examples of the testimony that is now deemed by the FBI as "erroneous"?

d. Have there been disciplinary personnel actions taken against the examiners who testified in those cases deemed problematic? If not, why not?

DNA

1. From Washington Post Article: The bureau has said it thinks the errors, which extend to 1999, are unlikely to result in dramatic changes that would affect cases. It has submitted the research findings to support that conclusion for publication in the July issue of the *Journal of Forensic Sciences*, the officials said.

a. In May 2015, the FBI Laboratory acknowledged errors in the original DNA frequency tables published in 1999 in the Journal of Forensic Sciences. Crime labs throughout the United States have used these DNA frequency tables to calculate statistics on DNA cases used in courts of law. At the time, the Bureau indicated these errors were unlikely to result in dramatic changes to statistics in DNA cases. After approximately six months, does the Bureau still find this true?

Anwar al-Awlaki

1. The Fourth Circuit recently remanded the case of Dr. Ali Al-Timimi on the basis that the government withheld evidence regarding the FBI's 2002 investigation of Anwar al-Awlaki. The FBI apparently instructed customs agents at JFK airport to release al-Awlaki, despite an outstanding warrant for passport fraud and despite al-Awlaki's link to four of the five hijackers of flight 77, which hit the Pentagon on 9/11. News reports intimate that there was an effort to recruit al-Awlaki as an asset. If this is true, clearly those efforts were unsuccessful as al-Awlaki went on to become the most notorious American al-Qaeda terrorist. Hindsight being 20/20, wouldn't we have been better served by holding al-Awlaki on the 2002 warrant?

Procurement

1. Reuters recently reported, "The U.S. Government Accountability Office on Tuesday upheld a protest by Harris Corp filed against the FBI's plans to award a sole-source contract to rival Motorola Solutions Inc for two-way radios under a larger umbrella contract." It was FBI's "second attempt to award a sole-source deal to Motorola." What is the FBI doing to ensure that its third attempt to contract for two-way radios does not run afoul of federal contracting rules?

Questions for the record from Representative Judy Chu (CA-27):

1. On or around May 21, 2015, Dr. Xiaoxing Xi, a U.S. citizen, was arrested for wire fraud in his home by approximately a dozen armed F.B.I. agents in front of his wife and two daughters. All charges against Dr. Xiaoxing Xi were eventually dropped. Because of his arrest and allegations of espionage, Dr. Xi's reputation has been tarnished, and he stepped down from his position as Chairman of Temple University's Physics Department. Can you share the details of his investigation and his arrest? What caused the investigation in the first place? What were the reasons behind the decision to send approximately a dozen armed F.B.I. agents to his home for his arrest?

2. On or around October 20, 2014, Sherry Chen, a U.S. citizen and employee of the National Weather Service in Ohio, was arrested by approximately six F.B.I. agents in her place of employment. What were the reasons behind the decision to send approximately six F.B.I. agents to her place of employment for her arrest?

Questions for the record from Representative Lamar Smith (TX-21):

Cyber Crimes

I represent San Antonio, known as Cyber City USA, where cyber security research, education, and development is vital to our local economy.

As Congress continues to discuss measures to combat cyber-crimes and proposals that promote the voluntary sharing of cyber threats amongst the private sector and with the government, some important questions remain.

1. What liability issues exist for parties who share information about cyber threats with each other and the government? This includes the critical infrastructure companies, such as the national utilities and their down-chain suppliers, whose equipment and services are directly targeted by cyber threats. What solutions are available to address the liabilities of those involved in the prevention of cyber-crimes?

2. Also, what privacy protections are in place for private sector organizations that share cyber threats with the government? Will the privacy of these entities' customers also be protected?

Questions for the record from Representative Ted Deutch (FL-21):

1. What were the quantitative metrics unearthed in the review after the Charleston shooting that suggested to you that the FBI needs to surge resources when conducting background checks? In other words, what share of those checks were getting completed, by when, what percent of total checks is ending up in the delayed/proceed category, and what share of those in the delayed/proceed category turned out to be prohibited, and for what reasons?
2. What did you mean when you said the FBI needs to surge resources and use better technology and innovation when conducting background checks?
3. What does the FBI think about benefits and obstacles to informing local authorities to investigate and retrieve delayed denials?

Questions for the record from Representative Trent Franks (AZ-08):

1. Historically, how many cases stemming from violations of the Partial-Birth Abortion Ban Act have led to FBI investigations and enforcement?

○