

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED FOURTEENTH CONGRESS FIRST SESSION

DECEMBER 9, 2015

Serial No. J-114-45

Printed for the use of the Committee on the Judiciary



*www.judiciary.senate.gov
www.govinfo.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

ORRIN G. HATCH, Utah	PATRICK J. LEAHY, Vermont, <i>Ranking</i>
JEFF SESSIONS, Alabama	<i>Member</i>
LINDSEY O. GRAHAM, South Carolina	DIANNE FEINSTEIN, California
JOHN CORNYN, Texas	CHARLES E. SCHUMER, New York
MICHAEL S. LEE, Utah	RICHARD J. DURBIN, Illinois
TED CRUZ, Texas	SHELDON WHITEHOUSE, Rhode Island
JEFF FLAKE, Arizona	AMY KLOBUCHAR, Minnesota
DAVID VITTER, Louisiana	AL FRANKEN, Minnesota
DAVID PERDUE, Georgia	CHRISTOPHER A. COONS, Delaware
THOM TILLIS, North Carolina	RICHARD BLUMENTHAL, Connecticut

KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

KRISTINE LUCIUS, *Democratic Chief Counsel and Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Grassley, Hon. Charles E.	1
Prepared statement	53
Leahy, Hon. Patrick J.	4
Prepared statement	58

WITNESS

Comey, James B.	6
Prepared statement	60
Questions submitted, classified responses received	79

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

WEDNESDAY, DECEMBER 9, 2015

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:01 a.m., in Room 226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley [presiding], Hatch, Sessions, Graham, Cornyn, Lee, Flake, Perdue, Tillis, Leahy, Feinstein, Schumer, Durbin, Whitehouse, Klobuchar, Franken, Coons, and Blumenthal.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman GRASSLEY. Before I give my opening remarks and Senator Leahy gives his opening remarks—and my opening remarks are a little longer than normal—I would like to say that there is a vote at 10:45, and I hope that between the Republicans and Democrats that we can keep the meeting going while we go over to vote at 10:45. That's my intention. And we'll have 7-minute rounds—7-minute questions for at least the first round. And if people want a second round, that is permissible.

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

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

At almost every turn, events have proven the President wrong about ISIS. In August 2012, he drew a “red line,” warning the Assad regime not to use chemical weapons in Syria. But the President backed down after Assad gassed his own people, and ISIS blossomed in the chaos that followed. In January 2012, the President referred to ISIS as a “JV,” or junior varsity. It promptly spent the next 6 months conquering territory across Syria and Iraq. In August of that same day, our President conceded that he didn't

have a strategy to defeat ISIS. A year and a half later, he remains without a coherent one. Even former Secretary Clinton admitted the other day that we're not winning the fight.

The President has been hoping that ISIS will go away because its existence does not fit a preferred political narrative. But hope is not a strategy. Hope is not a plan. And hope is not action. And all the while, the drumbeat of attacks on the United States continued. In May, there was an attack on a convention center in Garland, Texas. In June, police were forced to shoot a knife-wielding ISIS supporter on the streets of Boston. In July, we had the attack on military facilities in Chattanooga.

Director Comey, has, as of October, reported that the FBI was engaged in approximately 500-900 active domestic investigations against suspected ISIS-inspired operatives and other radicalized extremists. And he estimated that approximately 250 Americans have left the United States and traveled to Syria to fight with ISIS, or tried to do so.

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

Unfortunately, our President has responded to this crisis by trying to divide us, deride us, and distract us. In fact, he is doubling down on his strategy.

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

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

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

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

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

Our President has also continued to divide us, deride us, and distract us with the issue of gun control. To the President, radical Islamic terrorism is never to blame. But the constitutional right to own guns always is. But terrorists are not deterred by gun control. Strict European gun control laws did not stop the Paris attacks. California's assault weapons ban didn't stop the San Bernardino massacre.

Now, the Obama administration argues that allowing foreigners to buy guns who enter the United States through the Visa Waiver Program is a problem. I agree. But at the same time, the administration is apparently fine—fine—the outstanding is apparently fine with allowing refugees, asylees, and people on deferred action, and other noncitizens who are not legal permanent residents to buy guns. That makes no sense. With a few exceptions, we need to prevent all of these people from buying guns.

The administration's current fixation on guns and the Visa Waiver Program can be explained, though, because it is another area where the administration's actions have made Americans less safe. In fact, an opinion from Obama Justice Department required the Bureau of Alcohol, Tobacco, and Firearms to change its policies to permit persons arriving from visa waiver countries to buy guns, and the administrations removed the longstanding requirement that noncitizens at least establish residency for 90 days in the State where they want to purchase guns. These 90 days could be crucial in a terrorism investigation.

So, when we address the issue of foreigners in the United States buying guns, we need to be comprehensive about it, not just clean up the mess—not just clean up the mess that this administration created. Finally, our friends on the other side of the aisle have attempted to divide us, deride us, and distract us with proposals to deny the right to purchase firearms to those on various terrorist watchlists, including the No Fly List.

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

But the more fundamental point is: While these lists are useful in keeping us safe, they are the result of the Executive Branch's

unilateral decisions to put people on them without any notice or opportunity to be heard. As a result, they can be unreliable. And it isn't just constitutional to condition the fundamental right to keep and bear arms on an administrative list that lacks that kind of due process.

We would not consider conditioning any other constitutional right—such as the freedoms of speech or religion, or unreasonable searches and seizures—on such a process. That's why it is so surprising that this President, a former constitutional law professor, and so many of his political party would support such a scheme.

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

I also look forward to discussing a range of other issues with the Director today. One is the FBI's treatment of whistleblowers. I hope I have the support of the Director in strengthening the whistleblower law for the FBI. I also have questions about the FBI's investigation into former Secretary Clinton's email arrangement, the FBI's potential role in facilitating ransom payments, its use of spyware, and the ongoing efforts to correct injustices that result from flawed forensic work.

I apologize for a longer statement, but I also think that these are things that we don't discuss enough, and we have the opportunity today to discuss them. Now, it is Senator Leahy's turn, please. Take all the time you need, and I know you will, anyway.

[Laughter.]

**OPENING STATEMENT OF HON. PATRICK J. LEAHY,
A U.S. SENATOR FROM THE STATE OF VERMONT**

Senator LEAHY. The Federal Bureau of Investigation, as we know, is entrusted with the enormous responsibility of not only enforcing our laws but protecting the Nation. No matter what the threat, and no matter what the motivation of those threatening us, the FBI is told to keep us safe. On any given day, FBI agents around the country are investigating cases involving not only terrorism, but violent crime, gangs, cyber crime, identity theft, fraud, human trafficking, hate crimes, and child exploitation. And they know there is no simple answer.

For example, one of the greatest terrorist attacks ever in this country by Timothy McVeigh, none of us said after that, "Well, we have got to start excluding people who served in the military or people of Timothy McVeigh's religion." Instead, we went and found out what he had done and how we might stop others from doing the same thing.

The events of the past 6 months have underscored the varied nature of the threats the FBI faces. This past June, 9 African American churchgoers were murdered by a white supremacist during a Bible study in Charleston. The day after Thanksgiving, 3 individ-

uals—including a police officer—were shot to death inside a women’s health clinic in Colorado Springs. Last week, 14 county workers in San Bernardino were murdered in a shooting rampage. None of these seem related. All of them had different causes and motivations among those shooting. The Director may not be able to share all of the details about these investigations today, but I believe we can agree that there is one common motivating factor behind each of these heinous crimes, and that is, hateful extremism. The one in—the churchgoers who were murdered, the women—people in the women’s health clinic, and the people in San Bernardino, it was hateful extremism coming from different directions.

So, I think it reminds us to be vigilant against all forms of violent extremism. And I would hope that nobody underestimates the incredibly difficult job of protecting the country from terrorist threats. We can try to put all the blame on any one person, and that’s fine. But it’s not any one person. It’s all of us. We have to support the law enforcement and intelligence officials who work to protect our Nation by giving them the tools and resources they need to do their jobs effectively. And as we’ve heard from many law enforcement officials, we have to continue the very hard work sometimes of building trust in our communities among neighbors and with law enforcement so that we can all share in the responsibility of keeping our communities safe.

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

And if we give in to this sort of fear, then that way the terrorists and extremists win. They want us to be afraid; they want us to be a Nation divided. Groups like ISIS, for example, actively promote the narrative around the world that Muslims are not welcome in the United States. And certainly some of the—what I would call reprehensible and even unconstitutional comments by some allow them to spread that false notion around the world. When there is talk about rounding up all Muslim Americans or creating a registry based on religious beliefs or shutting our borders to all Muslims, that is the sort of xenophobic, hateful rhetoric that just plays into our enemies’ hands. It also demeans us as a democratic Nation founded on the principles of freedom, equality, and liberty. We Americans are better than that. Let’s not succumb to fear and give an image that is not the great country that brought my grandparents and my great-grandparents here.

We are a courageous and strong country. And our strength comes from our commitment to the morals and principles that continue to keep our country great—and a beacon of democracy to the rest of the world. The Senate at its best can be the conscience of the Na-

tion, and recent events demand that we start trying to be at our very best. We are not afraid of terrorists, and we not—should not let our country be defined by irresponsible fear-mongering.

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

I thank Director Comey for coming before the Committee today. I have known the Director for years. I know he shares my respect for the Constitution and my faith in the American people that we can rise above the divisive rhetoric of fear, because we are Americans. We should be better than that. And I believe we are. Thank you.

Chairman GRASSLEY. Since this is an oversight hearing, I would like to swear in Director Comey. Do you affirm that the testimony you are about to give the Committee—let me start over again. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Director COMEY. I do.

[Witness is sworn in.]

Chairman GRASSLEY. Thank you. I assume the Director of the FBI needs no introduction, but I would like to read a short introduction. It's a pleasure to introduce you to the Committee.

Director Comey became the Director of the FBI in 2013. He previously served as Deputy Attorney General and a U.S. attorney in New York and an assistant U.S. attorney in Virginia. He is a graduate of William and Mary and the University of Chicago Law School.

Welcome. Proceed with your testimony however long you want to take.

**STATEMENT OF THE HONORABLE JAMES B. COMEY,
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION,
WASHINGTON, DC**

Director COMEY. Thank you, Mr. Chairman, Members of the Committee. It's good to be back before you. As every Member of this Committee knows, the FBI has a very broad array of responsibilities to address a staggering array of threats that face our country in terrorism, in counterintelligence, and in criminal matters. The key to us doing that well is the great people of the FBI, and I so appreciate your support for them. They are the magic of the FBI. The best part of my job is to get to know those people and to watch them work. And so, I'm very grateful for the support of this Committee for those good folks.

What I thought I would do is start with our top priority, which is counterterrorism, and tell you how we're thinking about it and tell you a little bit more about how we are approaching the attack in San Bernardino.

The Members of this Committee know very well that the terrorist threat we face today comes at us from a number of groups, most prominently today from the group that calls itself the "Islamic State." The threat from the Islamic State has three dimensions.

One, they—they aspire to send operatives to attack the United States and its allies. Second, they aspire to attract people to come to their so-called caliphate to fight and achieve glory somehow from being in that savage place. And, last, where they can't send operatives or attract travelers, they hope to inspire or direct—and the two terms bleed together—people to engage in acts of violence in their home, to radicalize in their home, and to kill innocent people on behalf of these terrorist groups.

In Paris, we saw one dimension of that threat, which was the sending of operatives to attack and kill innocent people. In San Bernardino, we saw last week a different dimension of the threat, which is the homegrown violent extremist, the radicalizing in place in order to kill innocent people on behalf of a foreign terrorist organization, to claim a foreign terrorist organization and try to give it credit for acts of violence.

To find homegrown violent extremists, to find those that are radicalizing and being inspired by these terrorist groups is a very, very hard thing. All of you know from overseeing our work, we work at it every single day, and we use all the lawful tools that you've given us on behalf of the American people. Critical to our finding those people who are radicalizing in their homes is tips from the community. We have worked very, very hard to develop good relationships in communities all across the country, especially in Muslim communities, where we have terrific relationships, and those good people so often tell us when they see something that does not make sense. We are very grateful for that help.

We also want those folks to know that one of our responsibilities is to investigate civil rights cases and hate crimes, and we want people to know, if you think someone is terrorizing you or threatening you based on your national origin or your religion, please tell us so that we can investigate that. We are all in this together.

San Bernardino involved two killers who were radicalized for quite a long time before their attack. In fact, our investigation to date, which I can only say so much about at this point, indicates that they were actually radicalized before they started courting or dating each other online, and online, as late as—early as the end of 2013, they were talking to each other about jihad and martyrdom before they became engaged and then married and lived together in the United States.

We also believe they were inspired by foreign terrorist organizations. We're working very hard to understand exactly their association and the source of their inspiration. We're also working very hard to understand whether there was anybody else involved with assisting them, with supporting them, with equipping them. And we are working very, very hard to understand did they have other plans, either for that day or earlier, and that work continues.

Critical to that work is the support we get from State and local law enforcement through our Joint Terrorism Task Forces. Those 100 or so task forces are the backbone of this country's counterterrorism response. We are extremely grateful for the help from State and local law enforcement, and if you needed any confirmation of the quality and talent of the people in local law enforcement, you saw it that day in San Bernardino when highly professional officers stopped what might have been more tragedy, more violence.

As you mentioned, Mr. Chairman, I do want to give you a very brief report in my opening about where we are with respect to the challenge of encryption to our hardest work, to our counterterrorism work and to our criminal work. As you said, since we were last together, we have had good conversations with the folks in the tech sector in lots of different parts of this great country of ours, and those conversations have convinced me of two things, which are both good news.

The first is, we care about the same things. The tech companies and the FBI and everybody else involved in this discussion both care about safety on the internet. We understand that encryption is a very important part of being secure on the internet. We also all care about public safety. We also all see a collision between those things right now. We see that encryption is getting in the way of our ability to have court orders effective to gather information we need in our most important work, and we all agree we have to figure out whether we can maximize both of those values—safety and security on the internet and public safety. That's good news. We are not at war. We are about the same things.

The second piece of good news is all those conversations have actually convinced me it's not a technical issue. There are lots of folks who have said over the last year or so we are going to break the internet or we will have unacceptable insecurity if we try to get to a place where court orders are complied with. I actually think it's not a technical issue. There're plenty of companies today that provide secure services to their customers and still comply with court orders. There are plenty of folks who make good phones and are able to unlock them in response to a court order. In fact, the makers of phones that today cannot be unlocked, a year ago they could be unlocked. So, I really don't think it is a technical issue.

And people also, I think, better understand today the Government doesn't want a back door. The Government hopes to get to a place where, if a judge issues an order, the company figures out how to supply that information to the judge and figures out on its own what would be the best way to do that. The Government shouldn't be telling people how to operate their systems.

So, we are in a good place in terms of what we understand about our values. We are in a good place, I think, where we realize it is actually not a technical issue. It is a business model question. Lots of good people have designed their systems and their devices so that judges' orders cannot be complied with for reasons that I understand. I'm not questioning their motivations. The question we have to ask is, should they change their business model? That is a very, very hard question, lots of implications to that. We have to wrestle with it because of what's at stake.

I am limited in what I can say at this point about Paris and about San Bernardino, but let me give you a recent example.

In May, when two terrorists attempted to kill a whole lot of people in Garland, Texas, and were stopped by the action of great local law enforcement again, that morning, before one of those terrorists left to try and commit mass murder, he exchanged 109 messages with an overseas terrorist. We have no idea what he said because those messages were encrypted. And to this day, I can't tell you what he said with that terrorist 109 times the morning of that attack. That is a big problem. We have to grapple with it. And I very much appreciate this Committee's support for grappling with the hard questions around this. We must resolve the collision of those two values.

Then I will finish, Mr. Chairman—and I apologize for running over my time—with a word to the folks who may be watching us at home. I know, and the Members of this Committee know, how unsettling seeing this violence in Paris and in San Bernardino is to the good people of this country. My hope is that they will not allow themselves to be paralyzed by fear, but instead to channel that fear into something healthy, which is an awareness of your surroundings. In case after case after case, we see that when someone radicalized, somebody saw something, either online or in a school or at home, and didn't tell us about it. We hope that what people will do is not imagine these savages of ISIL or of al Qaeda as something bigger than they are, not imagine them in the shadows. That is exactly what these savages want. But, instead, simply be aware of your surroundings. If you see something, just tell us. We investigate in secret so that we do not smear innocent people. We will not race next door and bang on your neighbor's door. If no harm was there, no harm will be done. But if it was something, we may be able to stop something significant.

So, my request of the American people is don't let these savages paralyze you. If you see something that seems out of place, tell one of us. Thanks to the work of this Committee and a whole lot of people in our Government, we are better organized today than we were on September 11th. If you tell a police officer, if you tell a deputy sheriff you saw something that doesn't make sense, we will get it to the right place. We will check it out. We will see whether it was something.

You, I hope, will go on with your lives. You pay us to do counter-terrorism. We are not perfect. We are good at this. We cannot allow ourselves to be paralyzed by what these people are hoping to achieve. That is what I hope the American people will take from the unsettling experience of watching what goes on in San Bernardino and Paris.

With that, I apologize for going over my time, and I look forward to our questioning.

[The prepared statement of Director Comey appears as a submission for the record.]

Chairman GRASSLEY. No need to apologize for going over your time. And your reputation in both Republican and Democrat administrations is to call it like it is, and the American people are lucky to have a person like you particularly because you have a 10-year term to really do your job right.

Director Comey, earlier this week we learned that the National Counterterrorism Center has identified individuals with ties to terrorists in Syria who are attempting to enter the United States through the refugee program. You have acknowledged that there are gaps in the information that we—in screening Syrian refugees. But isn't it true that it's not just a lack of information that we have to worry about with people coming from Syria? After all, ISIS controls a large part of the country, including former Syrian government offices and facilities. Presumably, it has the personal information of many innocent Syrians. It has virtually unlimited funds.

So, now my question. Are you concerned that ISIS has the ability to create fraudulent passports or other identification documents for its operatives that has a practical—as a practical matter it would be almost impossible to detect?

Director COMEY. Yes, Mr. Chairman. The Intelligence Community is concerned that they have the ability, the capability to manufacture fraudulent passports, which is a concern in any setting.

Chairman GRASSLEY. Okay. The next point dealing with terrorists and the purchase of firearms, last week our President stated that there are individuals who can't get on planes, but they can go to a gun shop and buy a firearm, and there—and, quote, he said “nothing we can do to stop them.” But—and correct me if I'm wrong—the FBI is notified when someone on the terrorist watchlist attempts to purchase a firearm and a NICS check is requested, and the FBI has multiple avenues that they can pursue. These are some of these avenues. Delay the firearms transaction, and if the person is actually a terrorist, the FBI can arrest them for any crime for which there is probable cause; and, in addition, the FBI can intervene and directly confront the individual; the FBI can also put the suspect on what is called “around-the-clock surveillance.”

My question: Aren't these some of the tools available to the FBI to stop a suspected terrorist from buying a gun?

Director COMEY. Mr. Chairman, you are right, there are a variety of things that we do when we are notified that someone on our known or suspected terrorist data base is attempting to buy a firearm. The FBI is alerted when that is triggered, and then we do investigation to understand are there disqualifiers that we're aware of that could stop the transaction. And if the transaction goes through, the agents who are assigned to that case, to that subject, are alerted to it so they can investigate.

Chairman GRASSLEY. I thank you very much for that clarification. So, there are, then, actually many things that can be done, done right now, to stop someone on the No Fly List from buying a gun, and then that leads me to say that our President is misrepresenting the facts and misleading the American people on that point.

Next question. In July, you testified before this Committee about “Going Dark”—and you've already commented on some of this, but I want to be more specific—and Members from both political parties expressed serious concerns about the use of strong encryption by terrorists and criminals. I followed up with questions for the record, and I asked for data about the scope of the problem. At that time the administration declined to ask for a legislative solution and I asked for time to work with technology companies. But the

attacks in Paris and California have generated increased alarm about the problem.

So, question. When is the FBI going to respond to my questions relating to that hearing? And that's not the most important point that I am trying to bring out here. Could you update us about what is known about the role encryption may have played in these attacks? And I know you have already said that you are limited in what you can say, but whatever you can tell us, do it. And, finally, what is the state of your conversations with the technology companies to address that problem? And you may have expressed that in your opening statement, the last part.

Director COMEY. Thank you, Mr. Chairman. At your request and the request of other Senators, we are collecting data concerning the ways in which encryption is affecting our ability to implement court orders for data in motion—that is, emails or phone calls—and data at rest that is sitting on devices. And I don't know exactly when we are going to get that to you, but that work is in progress, and it will show there is a significant impact, and growing, across our work, both terrorism and in criminal cases.

With respect to our conversations with the—well, first of all, the second piece. With respect to its role in cases, I don't want to talk about Paris yet or San Bernardino because we are doing a lot of work with respect to those now. There is no doubt that the use of encryption is part of terrorist tradecraft now, because they understand the problems we have getting court orders to be effective when they are using these mobile messaging apps, especially that are end-to-end encrypted. We see them talking about that all over the world. It is a feature especially of ISIL's tradecraft.

Last, the conversations with the companies have been good. Like I said, they really have made clear to me that we are not at war with each other; we care about the same things. It's also made clear to me that it is really not a technological problem. We are not going to break the internet or expose us to tremendous insecurities of different kinds by requiring—getting to a place where companies comply with court orders, because lots of good companies do today. It's a business model question. Good people have made a decision to design products and sell products where court orders are ineffective. And I'm not impugning their motives. I understand they see it as a competitive issue or they think it is just the right thing to do.

The question we have to ask ourselves is. Is there a way to get folks to change their business model so that judges' orders will be complied with? And if that can't be done voluntarily, what are the other alternatives? And these conversations continue within the executive branch and with our private sector partners.

Chairman GRASSLEY. I could start another question now, but it would take too long for you maybe to answer, so I think I will go to Senator Leahy so we can kind of keep on time here.

Senator LEAHY. Thank you, Mr. Chairman.

I just want to follow-up on a question that Senator Grassley asked you about the FBI being notified if somebody on a No Fly List or that type of list was buying a weapon. If they buy it at a gun show where there is no reporting of it, you are not notified, are you?

Director COMEY. That's correct.

Senator LEAHY. And if they buy it on an internet sale, you are not notified, are you?

Director COMEY. Correct.

Senator LEAHY. And even if they go to a gun dealer who has to notify you, you are notified, but there is not an awful lot you can do about it. Is that correct?

Director COMEY. Unless, as I said, we find some disqualifier under the law. But if we do not find one of those things, there is nothing we can do to stop it.

Senator LEAHY. So, the President's statement that somebody on a No Fly List or on these watchlists can go and buy weapons in the United States is correct.

Director COMEY. There is no prohibition connected to the No Fly List. That's correct.

Senator LEAHY. Thank you very much. I just wanted to make sure that was—that was clear.

Now, right after you were confirmed, you spoke about the detrimental impact of sequestration and the hiring freeze on criminal and counterterrorism investigations. I happen to agree very much with what you said. I understand you are still in the process of trying to replace all the agents that were lost due to sequestration. Is that correct?

Director COMEY. That is correct. We are still trying to dig out of that hole.

Senator LEAHY. So, when you can finally hire, you have got to train them. Then you have got to get them into investigations. So, this sequestration—I don't want to put words in your mouth, but is that having a long-term effect on the FBI's ability to fight crime and terrorism?

Director COMEY. Yes.

Senator LEAHY. And what would be the impact on the FBI if Congress could not come to an agreement on an omnibus appropriation bill and instead just passed another long-term spending resolution?

Director COMEY. Well, if we return to the impacts of sequestration that were kicking in when I started this job, it would be a disaster because we are just digging out of the hole. To return to a place where we have to ration gas and shut down Quantico and choose which people to interview based on how much gasoline we have in our tanks, that doesn't make any sense to me. So, it would be a big, big deal.

Senator LEAHY. Without going into them here, I remember some of the worst-case scenarios you described to me privately, and they are chilling.

Now, we have had a lot of talk about our refugee system. I just want to clarify a few facts. The refugee program presents the longest and most complicated path for entering the United States, and refugees do not get to pick which country they are sent to. They are vetted more intensely than any other category of traveler. The vetting is conducted before any refugee can get on an airplane to come here. The process can take years. That's why I agree with former national security leaders like General Petraeus and Secretary Hagel and General Brent Scowcroft, who wrote to Congress

that turning our backs on refugees would be contrary to our Nation's tradition of openness and inclusivity and would undermine our core objective of combating terrorism.

Now, the House has just passed a bill that would require you to personally review, along with the Secretary of Homeland Security and the Director of National Intelligence, each and every refugee application. Is that really feasible?

Director COMEY. Well, first of all, if the intention is for me to do it personally, that would be very, very hard. But even as I understood the ask, it was, could I certify to there being no risk associated with an individual. And, again, the Bureau does not take positions on legislation, and we do not get involved in policy decisions. But that practically would be impossible.

Senator LEAHY. So, it would make our refugee program impossible also.

Director COMEY. Logically, if someone could only come into the country if I were to certify to that, it would—it would.

Senator LEAHY. Thank you. We often hear from law enforcement that hateful and ignorant anti-immigrant rhetoric undermines community trust and ultimately harms the ability of law enforcement to do its job. I have the same concern when we hear some say we should close our borders to all people of a certain religious faith or track people because they have certain religious beliefs.

I worry that these kinds of proposals feed what are the real lies that ISIS spreads, that the U.S. is anti-Muslim, and they use that as a tool to recruit new members. Is that correct?

Director COMEY. The notion that the U.S. is anti-Muslim is part of ISIL's narrative and al Qaeda's narrative and other terrorist groups.

Senator LEAHY. Thank you. Earlier this year, this Committee in a bipartisan fashion approved a sentencing reform bill that reduces—it does not eliminate but reduces some mandatory minimum sentences. As I have said oftentimes publicly, I would like to see an end to all mandatory minimums, but at least this is a good step in reforming our criminal justice system.

Attorney General Lynch, Deputy Attorney General Yates, former Attorney General Michael Mukasey, and other law enforcement leaders have stated their support for this compromise bill. Do you agree that it strikes a reasonable balance?

Director COMEY. Well, Senator, as you know, we don't take positions on legislation, but because I spent my career as a prosecutor, that's an area of interest of mine. I actually read the bill, and my reaction was it's reasonable; the things that are discussed in there are reasonable. I have found mandatory minimums—and we may disagree on this. I have found mandatory minimums to be an important part of making some of the most important cases I was involved with. But I think that the reform, as I understand it, seems reasonable to me.

Senator LEAHY. The Fraternal Order of Police has strongly opposed adding a mens rea provision to this. We don't have one in the bipartisan bill which was negotiated, Republicans and Democrats. They say such a provision in this bill—it doesn't mean we can't look at mens rea in other criminal bills, but in this one, it would be a poison pill. Do you have any views on that?

Director COMEY. I don't. I know it is a subject of interest. I do not know it well enough to comment. In fact, I was racking my brain. I don't think I ever prosecuted a case that did not involve a mens rea requirement, so I don't know enough to say.

Senator LEAHY. And, last, I keep pushing for the bulletproof vest partnership bill, which Senator Campbell of Colorado and I started. You have the resources to equip your agents with body armor, but would you agree that it is really important that local law enforcement have body armor?

Director COMEY. Very much.

Senator LEAHY. Thank you. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Leahy, you probably asked the right question and the Director answered it right, but also the Director answered my question right about whether the President was misleading, and that's because in the President's televised address—and I think it was thoroughly vetted—he stated that someone on the No Fly List could walk into a gun store and buy a gun and there was nothing that could be done about it. So, the President said nothing about going to a gun show or the internet to buy a gun, and the Director agreed with what I said about that at that time.

Now, the order is going to be——

Director COMEY. Mr. Chairman, could I——

Chairman GRASSLEY. Yes.

Director COMEY. I just want to make sure that I was not heard to be saying I think the President was misleading. I am not trying to take shots at anybody. I was trying to answer the questions about what are our capabilities in that regard.

Chairman GRASSLEY. Thank you very much. I made the statement. You didn't make it.

The order at the fall of the gavel is going to be Graham, Cornyn, and Lee, and then after the gavel came down, Hatch, Flake, Perdue, and Sessions. And then I will have Senator Leahy tell me who the next Democrat will be.

Senator LEAHY. That would be Senator Feinstein.

Chairman GRASSLEY. Senator Feinstein after Senator Graham.

Senator GRAHAM. Thank you, Mr. Chairman.

I want to echo what the Chairman said about your service as FBI Director. I think we are lucky to have you. If I buy a gun on the internet, is it delivered to my home?

Director COMEY. If you buy a gun on the internet?

Senator GRAHAM. If I try to buy a gun on the internet, where do I pick it up?

Director COMEY. I assume it is shipped to you, but I don't know for sure, actually.

Senator GRAHAM. Okay. Well, let's find out the answer to that.

Okay. Do you agree with the following statement. There are more terrorist organizations with men, equipment, and safe havens along with desire to attack the American homeland any time since 9/11?

Director COMEY. I agree.

Senator GRAHAM. So, do you agree that the budget cuts that Congress has imposed in the past has reduced your ability to defend this Nation?

Director COMEY. I agree.

Senator GRAHAM. Do you believe that the budget cuts that will go back into effect in 2 years will dramatically harm your ability and your agents' ability to defend this Nation if sequestration kicks back in?

Director COMEY. I agree.

Senator GRAHAM. Thank you. All right. Do you agree that rhetoric coming from political candidates running for President wanting to shut America down based on someone's religion empowers the enemy?

Director COMEY. I'm trying to avoid taking shots at anyone, as I said. I—

Senator GRAHAM. Well, just strike "Presidential candidates" and put a widget.

Director COMEY. I do believe that our ability to get cooperation in the United States, which is my primary responsibility, our primary responsibility, depends upon people trusting us and having a level of comfort with us. And estrangement gets in the way of that.

Senator GRAHAM. Do you agree with me that if you are a soldier, diplomat, or FBI agent serving in the Mideast right now, the fiery rhetoric from here at home can put you in jeopardy?

Director COMEY. People who know better than I have said that, and so I credit that.

Senator GRAHAM. Was the woman shooter in San Bernardino radicalized before she came to America?

Director COMEY. It looks like she was. So, far the data we have collected, the intelligence indicates that she was before she connected with the other killer and came here.

Senator GRAHAM. Is there any evidence that this marriage was arranged by a terrorist organization or terrorist operative? Or was it just a meeting on the internet?

Director COMEY. I do not know the answer to that yet.

Senator GRAHAM. Do you agree with me that if it was arranged by a terrorist operative or organization, that is a game changer?

Director COMEY. It would be a very, very important thing to know. That is why we are working so hard to understand it.

Senator GRAHAM. Well, that is the biggest focus, I think, of how it would change the game, that they could actually arrange a marriage of two like-minded individuals, use the fiancé visa system to get into the country. So, that is a good answer. ISIL—is it their goal to strike the American homeland?

Director COMEY. One of their goals, yes.

Senator GRAHAM. Yes, not their only goal, but it is one of their goals. Is that correct?

Director COMEY. That's correct.

Senator GRAHAM. Do you believe ISIL cells are already here in America?

Director COMEY. I don't have reason to believe that. It's something that we constantly look for, and—

Senator GRAHAM. Do you have any doubt they are trying to create one if they do not have one today?

Director COMEY. No. They are trying to do two things. They're trying to motivate people already in the United States to become killers on their behalf, and they would very much like to, as they

aspire to be the leader in the global jihad, send people here to conduct attacks. It's that second piece that we have not seen yet.

Senator GRAHAM. And that's what you have to guard against every day. I mean, they have to be right only once. You have to be right every day.

Director COMEY. That is right.

Senator GRAHAM. And the less resources you have and the harder time, the longer it takes you to find out what is going on. If you can't listen to the conversations in a constitutionally appropriate way, then the enemy has an advantage over you, is that correct?

Director COMEY. Correct.

Senator GRAHAM. Is it fair to say that they wake up every day in Iraq and Syria thinking about ways to hit us here?

Director COMEY. Some of them do for sure.

Senator GRAHAM. Is it fair to say that the Paris attack was a very sophisticated, well-planned attack that came from Syria?

Director COMEY. Yes.

Senator GRAHAM. Is it fair to say that those people who planned the terrorist attack would hit us here at home if they could?

Director COMEY. Yes.

Senator GRAHAM. How many countries does ISIL have a presence in?

Director COMEY. Sitting here, I can't give you a precise count, but it is—

Senator GRAHAM. More than Syria and Iraq?

Director COMEY. Oh, certainly.

Senator GRAHAM. I think there are a couple thousand now in Libya that took Qaddafi's hometown.

Director COMEY. They claim branches in more than five, between five and ten. And the question of whether they have a presence is obviously something we're focused on here. But it is more than five.

Senator GRAHAM. Can you give us any time period of when you think ISIL will be destroyed?

Director COMEY. I cannot.

Senator GRAHAM. Can you think of any means that we should take off the table that is constitutional in terms of fighting ISIL? Is there anything you want to take off the table in terms of fighting ISIL as long as it meets our constitutional requirements?

Director COMEY. I think I am only qualified to speak about the world that the FBI sits in, and we use all lawful tools that Congress gives us to try and meet this threat. So, I would not take any tool off the table that is lawful.

Senator GRAHAM. Right. And when it comes to tools, you are using all the ones you have because this is a very consequential fight.

Director COMEY. Yes.

Senator GRAHAM. What do you think the likelihood of another 9/11 against the homeland will be if we don't destroy the caliphate in Syria and Iraq in the next year?

Director COMEY. That's certainly a hard question for me to answer. Their ability to have a safe haven from which to gather resources, people, and plan and plot increases the risk of their ability to mount a sophisticated attack against the homeland.

Senator GRAHAM. So, the best strategy would be, at least in the short term—they are large, they are rich, they are entrenched—is to make them small, poor, and on the run. Would that be a good approach to ISIL?

Director COMEY. That makes sense, and my understanding is that is the aim.

Senator GRAHAM. Is it fair to say that other countries want to help America in this fight, we don't need to go it alone?

Director COMEY. Certainly in dealing with the FBI, we get tremendous cooperation from a whole lot of countries. So, yes, they are like-minded.

Senator GRAHAM. What country has the most gun control laws—France or the United States?

Director COMEY. I don't know.

Senator GRAHAM. Would you check into that?

Director COMEY. Sure.

Senator GRAHAM. Because I just want everybody to know that gun control is as legitimate debate here at home. It is not part of a strategy to destroy ISIL, that the laws in France are very robust, but terrorists got the weapons. Don't mix the two. Thank you very much, Mr. Director.

Senator HATCH [presiding]. Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Senator Hatch, and welcome, Director Comey, and thank you very much for your good work.

I was just reading a report, "ISIS in America," Program on Extremism from George Washington, where they say that 71 individuals have been arrested on charges related to the Islamic State since March 2014 and 56 of them this year alone. Is that correct?

Director COMEY. I do not know whether the precise numbers are right, but roughly, that strikes me as correct.

Senator FEINSTEIN. Okay. The last time you were here, you mentioned that you have an investigation going in every FBI field office on this—in the country. Is that correct today?

Director COMEY. Yes.

Senator FEINSTEIN. Okay. I wanted to ask you—I was at home and I was watching on television when I saw press and others going through the apartment of the couple in San Bernardino that committed this terrible act. And I was appalled that it was not taped off because, from an intelligence point of view, it immediately compromised any future intelligence gathering from any trace materials or anything else. How did that happen?

Director COMEY. A lot of folks, I think, found that confusing. That is our—our, what I believe, great criminal justice system in action in part. The way it works is we get a search warrant that allows us to enter someone's residence. Our forensic experts and agents were in that residence for over 24 hours and combed through it and took everything that we could take under the search warrant and that was appropriate to take and recorded that which we needed to record.

Once we have exhausted that examination, we board the place up and make it secure. We have to post under the law an inventory of what was taken—that is part of American law—and then leave the residence. That part makes good sense to me. The part I cannot

explain is why the landlord for the place allowed the boards to be pried off and folks to go through.

Senator FEINSTEIN. Well, let me stop you. Wasn't it important enough to have some law enforcement officer there to see that that did not happen? I mean, after all, you know, 14 people were killed and 21 were injured. It seems to me that protecting that scene is really important. So, I hope that there is some procedure whereby that doesn't happen again.

Director COMEY. Well, the judgment of the investigators and our forensic experts was we were done with that scene. There was nothing else to be gained from that scene, which is why it was boarded up, and then the inventory was left. What happened next was strange and it struck me as strange on the TV that the landlord allowed the media to go through. But we had done our work in a careful, responsible way. Twenty-four hours is a long—

Senator FEINSTEIN. Does it go back to local police jurisdiction?

Director COMEY. No. It goes back to the owner and lawful occupant of the residence.

Senator FEINSTEIN. So, you relinquish the premises regardless of whether somebody finds something that they want to come back and look for?

Director COMEY. No. If there is a need for the investigation to continue to have access to the place, we will preserve the scene. We will put up crime scene tape. We will post a guard on it. But if we are done with someone's residence that we have searched, under the law we return it, and we post an inventory inside as to what was taken.

Senator FEINSTEIN. Oh, boy. Well, maybe we can talk a little bit about that, because from an intelligence point of view, I could see things in an investigation that would crop up that you might want to come back and look behind the picture frame on the wall because there is some message behind the picture that you do not know about when you went through the apartment initially, or some document. So, it just does not seem to me to be smart, but let me go on.

With respect to encryption, Senator Burr and I on Intelligence are working on this issue. I can tell you that when I went and visited with the chief counsels of the big tech companies in my State about trying to get a bomb-making portfolio of 15 pages off the internet—this was the bomb that goes through a magnetometer, and I pointed that out, and I pointed out it had been tested. And there was no interest in taking it down. One company said, Twitter, "If we find something, we take it down, but we don't report it." In the intelligence bill which passed the Senate, this was taken out later and a need to pass the bill by unanimous consent.

We also had legislation that said that if you find terrorist information, you must report it to law enforcement. Would you support that?

Director COMEY. I know the administration, the Justice Department, is formulating a view on that, and so that's for them to do. Operationally, it wouldn't have any bad impact on the FBI, and so I guess I have got to wait—

Senator FEINSTEIN. Well, the FBI would not want law enforcement to know what is being said on the internet that is terrorist-

related or has complicity to commit an act—I should say conspiracy to commit an act?

Director COMEY. No, the more we know, the better.

Senator FEINSTEIN. I would think so.

Director COMEY. But I'm not in a position to offer a view on whether the Justice Department will support the legislation itself, I guess is what I am trying to say.

Senator FEINSTEIN. Okay—okay, fine. With respect to what you said on encryption, that you don't want a back door, you don't want keys, it seems to me that the probable cause warrant process is the best process. You said here today enough to indicate that you would support that. Is that correct?

Director COMEY. I am sorry. Support? I am not following—support.

Senator FEINSTEIN. Legislation which enabled a warrant with probable cause to be able to look into an encrypted web, which you said the companies told you was possible.

Director COMEY. Right. It's possible lots of companies do it today, provide secure services and comply with court orders. There are others who built their business models so that they say, "Even if we want to, we can't." But the question of whether the answer is compelling them to do that by legislation is one that I can't answer sitting here. I think that is something the administration a couple months ago decided not to seek legislation now, but I also know there is continuing to be conversations inside the administration.

Senator FEINSTEIN. Well, I am going to seek legislation, if nobody else is, and I think—I know Senator Burr thinks somewhat similarly. I'm very concerned about it because when I met with high tech, what they told me was there are parts now—when you talk to us about the dark web, which is listened to very carefully—that they cannot unencrypt. And I can give you the names of the companies that said that to me. And I have real concern about that. You know, I have concern about a Playstation which my grandchildren might use and a predator getting on the other end talking to them, and it is all encrypted.

And so, I think there really is reason to have the ability with a court order to be able to—and if you have cause to believe that criminality may be going on, to be able to get into that. I suspect what happened was in the aftermath of Snowden, particularly Europe got very conservative with respect to encryption, and the companies back away. Now, that's changing with Paris and, God forbid, what might happen in the future.

So, what I'm trying to say is, I think, this world is really changing in terms of people wanting the protection and wanting law enforcement, if there is conspiracy going on over the internet, that that encryption ought to be able to be pierced. Do you agree?

Director COMEY. I agree. I would very much like to get to a world where if a judge issues an order, companies are able to comply with it, either to unlock a device or to provide the communications between terrorists or between drug dealers or kidnappers. I very much would like to see that.

Senator FEINSTEIN. Good. Thank you very much. Thank you, Senator.

Senator SESSIONS. Thank you, Senator Feinstein.

Director COMEY, thank you for your leadership. I believe you are a person that is well qualified for this job and understand the seriousness of your role and have the background and experience to do it well.

You know, you testified before the House Committee on October 22nd, and you said, dealing with prisons and punishment, you struggle with the term “mass incarceration,” quote, “because it conveys a sense that people are locked up en masse, but in reality, every case is individual. Everyone has a lawyer, everyone has a judge, everyone had to be proven guilty.” And isn’t it amazingly true that we now over 95 percent of criminal defendants plead guilty in Federal court?

Director COMEY. The days of trials seem to be bygone.

Senator SESSIONS. So, I think that’s a testament, don’t you, to good investigation and solid cases that are being brought?

Director COMEY. I think at least, in part, that is driving it.

Senator SESSIONS. I think so, too.

Now, since I was prosecuting, maybe since you were prosecuting, the Guidelines—Sentencing Guidelines under the Supreme Court have become advisory, not binding. Attorney General Holder has altered traditional Department of Justice policy and declared that prosecutors don’t have to charge the most serious offense. The Sentencing Commission has reduced the guidelines that were in their power to do so. Senator Durbin and I worked together on legislation that reduced the penalties for crack cocaine rather significantly, more than a lot of people understand. And now we are considering additional reform in sentencing.

You said, I thought wisely, that—you expressed concern about the increase in violent crime and murders around the country. Instead, it would prompt you to be, quote, “thoughtful” about criminal justice reform proposals and noted, quote, “We have hit historic lows in violent crime recently, and if we let it slide back, we will need to explain to those that come after us what we did or did not do to let that happen,” close quote.

Would you explain the trends in crime and punishment and why you shared those words?

Director COMEY. What I was getting at, Senator, is our world, with respect to violent crime, is a world that was hard to imagine 25 years ago, and a whole lot of hard work went into getting us to historically peaceful America. And a big part of that, I believe, was law enforcement’s work, and I also believe every sentencing I ever went to in a way was a tragedy because a life was being wasted. But that work had to be done to protect those neighborhoods. And what I was urging folks to do—I think Harry Truman said, “The only thing new is the history you do not know”—is for folks just to remember we used to be in a very different place, and there are reasonable reforms, as I said earlier, we can—we can put into place. But we have to remember where we once were, and I would not want to do anything without understanding the history that lets us slide back to that place. And I was saying that in the context of a worrisome spike in homicide in over 30 of the Nation’s top 50 cities that has occurred this year that is hard to explain, but it is very worrisome. And I was simply sounding an alarm saying we have to talk about this, because we have gotten to a great place

in this country, and this is worrisome, and it drives us to need to be even more thoughtful about how we change our criminal justice system.

Senator SESSIONS. Well said. I think this is—I was there when the crime rate was high, and I have seen it decline as a prosecutor and subsequent to my time, and we have made real progress. I have a chart that shows the Federal prison population and how it has been developing, and I hope my colleagues will look at this chart, because we have the perception that the Federal prison population is surging. But, in fact, it peaked around 2013 or so, and it has been declining steadily ever since. And according to the Bureau of Prisons, they project the population in Federal prisons this year to drop by nearly 15,000 additional. So, we are just not on a trend to mass incarceration and a surging Federal prison population.

[Poster is displayed.]

What about State prisons? There are many, many more in State prison than in Federal prison, maybe 10 times or more. Let's see what is happening in the State systems. We have seen a rather dramatic decrease in penalties in States, and part of it is budget driven. And people then begin to develop theories to justify a reducing prison population based on budgets, and you have also a lot of people have always doubted the value of prison. So, we've seen a substantial decrease in State prisons, and I think that will continue. And so, I guess—and since we know there is a pretty high recidivist rate for prisoners—and I am not trying to put you in a big argument here, but the fact is that more people that are released from prison, aren't they likely—aren't we likely to see an increase in crime because the recidivist rate—rate remains high?

[Poster is displayed.]

Director COMEY. I am not an expert. As I think you said, the logic of it would say yes, there would be—given the recidivism rate, which is one of the things that is exciting, I think, about the legislation Senator Grassley talked about, it tries to get us doing a better job at reducing recidivism. But the math would say sure.

Senator SESSIONS. Here the Association of Assistant United States Attorneys wrote a letter and said this: “Every incremental weakening”—questioning plans to further reduce sentencing, “Every incremental weakening of those mandatory minimum penalties will have a corresponding impact on the ability to successfully investigate and prosecute drug trafficking. The current proposal will significantly weaken the mandatory penalties and significantly deprive law enforcement authorities and prosecutors of the tools they need to successfully address drug trafficking.”

Now, you said you could accept the changes, but that's a statement that is worthy of serious evaluation. Would you agree?

Director COMEY. Sure.

Senator SESSIONS. Thank you, Mr. Chairman.

Chairman GRASSLEY [presiding]. I have been told by Democrat staff that Senator Whitehouse is next.

Senator WHITEHOUSE. Then I will go next. Thank you, Mr. Chairman. Welcome, Director Comey. As the author with Senator Cornyn of the title you just said was exciting, I thank you. I want to ask you about two things. One is botnets, and the other is to fol-

low-up on Chairman Grassley's and Senator Feinstein's concerns about encryption of communications.

Botnets first. Senator Graham and I have a bill that tries to enhance the Department's authority to pursue the civil remedies that have allowed the Department of Justice to pull down botnets. One of the challenges that that effort has faced has been the legal requirement that the botnets have to be engaged in fraud and—or wiretapping before the Department can go and pull them down.

My sense is that a botnet is essentially like a weed. There is no such thing as a good botnet. They are either actively doing evil things, or they are a latent mechanism for doing evil things later on, and that a more vigorous effort to root them out of the internet and create better internet hygiene against botnets would be a good thing.

Now, when—I had a vote organized, and there were various machinations in the Senate that prevented the botnet provision from coming to a vote. And behind that were some statements that I'm a little bit astonished by, but basically that some botnets are actually good and we should protect them out there. I see you looking very surprised.

Let me ask you, could you react to that? Do you think I am in the right place on this, that a botnet is either a latent or an active menace on the internet and that we should be aggressively taking them down?

Director COMEY. I had that facial reaction because I don't know of a good botnet. Botnets are armies of zombies, so whether they are coming at you or whether they are standing still, it is still really bad. I don't know of a good purpose for an army of zombies.

Senator WHITEHOUSE. Thank you very much. I appreciate it. I am glad we are on the same wavelength.

With respect to encryption, we talk about it often as a technical question, and let me be the first to say I don't want a Government back door either. Nobody wants a Government back door. But as you say, when it's the business model of a particular company to disable its own ability to comply with a properly authorized subpoena or search warrant under our laws, that is a very different proposition, and it is that proposition that I want to speak to. And I would like to ask you to talk about two things.

The first is, from the FBI's perspective, what do you think are going to be the worst and most dangerous consequences of that encryption propagating and criminal use of it or terrorist use of it? And less from the FBI's perspective but more generally, since the FBI is a leadership organization within law enforcement, what do you think regular police departments and law enforcement officials around the country are most likely to see as the hazards of this encryption in their efforts to protect the public? So, first the FBI, and then more general law enforcement concerns.

Director COMEY. From the FBI's perspective, we are increasingly seeing, inevitably we'll see entirely that criminals and terrorists and spies have an unparalleled ability to communicate with each other worldwide. Increasingly, we are unable to see what they say, which gives them a tremendous advantage as against us.

In the good old days, it was harder for them to communicate with each other. Today they have a tremendous ability. Our ability

to monitor them has not kept pace; in fact, it is going in the wrong direction. So, our ability to find people hiding in the United States looking to do bad things to root out all kinds of organized criminal actors is steadily being impaired. That's the problem.

State and local law enforcement, the impact is for them almost entirely devices that cannot be opened with a search warrant. And I do very much agree it is a business model choice, because the folks who are today selling those phones, a year ago their phones did not have that capability. I do not remember anybody saying, "I am not buying their phones because they are insecure." It is not a security issue. It is a business model issue, and there are good motivations behind that. But we have to talk about those, and so they are encountering increasingly, in kids missing cases, in drug cases, in violence cases, devices that are a brick to them that hold all of the evidence that might help them figure out where a child is, untangle a kidnapping, or figure out where a drug gang is operating. That's their problem, less the data in motion problem for the State and local, but increasingly this it cannot reach the evidence that a judge would otherwise authorize them to get.

Senator WHITEHOUSE. That's very compelling testimony, and I can share with you that the Chief of Staff to the President of the United States has said that to me that one of the things that keeps him up nights is this encryption problem. My concern is if these companies have already made the decision that it's their business model to prevent law enforcement from using subpoenas and search warrants in the traditional way, then they have a business justification in their minds for doing it. And if that's their position, how is talking to them going to change that. Where is the leverage point? What is the administration's process for trying to solve this problem?

Director COMEY. I don't know that there is a leverage point that is going to flip it from one side to the other. I do think that all businesses are making trade-off decisions, and at least, in part, what has motivated some of the companies to switch to this default encryption is they believe—and I'm not questioning their good-faith belief—that it's a competitive imperative, that customers want this. And so, the conversations are useful because I think we can show them there is tremendous harm associated with this, and the customers increasingly see that, and so my hope is they will see that calculus differently, and their customers will speak to them and say, "No, I'll keep using your phone. It is a great phone, even if you would allow a judge to issue an order to unlock it in a terrorism case or in some other criminal case."

Senator WHITEHOUSE. And, presumably, if you could show that but for the phone having been turned into a brick as a result of the company's business practices and been protected from search warrants and subpoenas, a child was—could not have been rescued who otherwise could have been, and there is a fatality that has resulted, presumably they would see that as something less than great publicity for their choice.

Director COMEY. Well, I actually—I mean, I wasn't just saying this. They do care about public safety. These are good people. What the conversations have helped them understand is the darkness that we see. Good people don't spend all day long worrying about

the things I worry about. What the conversations have helped them see is, “Wow, there really is a real-life impact to this.” We’re trying to find terrorist needles in a haystack. When we find one, it goes invisible because they are using end-to-end mobile messaging apps. That has real consequences. These good people see that. That’s where the conversations have helped. Now, where that is going to lead, I don’t know yet.

Senator WHITEHOUSE. Thank you. If we can help in any way, please call on us.

Chairman GRASSLEY. Senator Lee is next, but before you go, unless Durbin and Schumer come back, it will be Klobuchar and then the other Senator from Minnesota.

Senator FRANKEN. That is fine. That is who I am.

[Laughter.]

Chairman GRASSLEY. And the reason I took time to do that, I am going to go up to Budget and ask a question, so I hope everybody will observe the 7-minute rule we have.

Senator LEE. Thank you, Mr. Chairman. As the other Senator from Utah, I am happy to comply with the 7-minute rule.

Thank you, Mr. Comey, for being here with us today. Thanks for all you do to keep us safe. There has been some discussion and a little bit of confusion lately about the USA FREEDOM Act. In part, this has been precipitated by some of the discussions going along with the Presidential election cycle that is in full tilt now. But, to clarify, I have just a few questions about the USA FREEDOM Act and how it operates.

First of all, the USA FREEDOM Act doesn’t prohibit the Government from gaining access to telephone metadata, correct?

Director COMEY. Correct.

Senator LEE. It allows the Government to get metadata, telephone records, connected to any terrorist investigation, such that if the Government wants to gather metadata connected to a particular phone number that it believes is connected to a terrorist investigation, the Government can get that.

Director COMEY. Correct.

Senator LEE. And the USA FREEDOM Act does not affect in any way the Government’s ability to gain access to any metadata that either originated—as to a phone call that either originated outside the United States or that originated here and was directed outside the United States.

Director COMEY. Correct.

Senator LEE. Did the enactment of the USA FREEDOM Act substantially affect the Government’s ability to prevent the San Bernardino attack?

Director COMEY. I’m only hesitating because I don’t want to talk about particular techniques we are using to understand that attack. And so, I guess, Senator, I need not to talk about it in the context of that case.

Senator LEE. Okay. I would note here only that it is significant that only—only 4 days prior to the attack the Government had access to all of the records that it had access to—that it had access to for years prior to the passage of the USA FREEDOM Act because there was a 6-month moratorium between its passage and it kicking in. And I personally consider that highly unlikely, some

would say mathematically impossible, that it had any difference there. And certainly the Government can still investigate the San Bernardino attack by going after records of the individuals suspected to be involved in that attack.

Director COMEY. Sure.

Senator LEE. Thank you. I want to talk a little bit about this encryption issue. I was pleased to hear you say—and I hope I understood you correct—that you’re not pushing for legislation that would mandate tech companies to put a back door, to develop a back door and make that available.

Director COMEY. Correct.

Senator LEE. What you were saying, as I understand it, is that some companies, many companies, could choose voluntarily to assist law enforcement in the execution of a warrant in helping gain access to any information that they might have access to.

Director COMEY. Correct, and those are the conversation we have been having.

Senator LEE. And so, but I assume in order to do that, would they have to develop their own back door that they could use internally?

Director COMEY. Well, I don’t know what in that context the term “back door” means. They would have to figure out how, consistent with their security requirements, they could comply with the judge’s order, as a lot of companies do today. So, they would have to figure out under our system what would be the best way to comply with the judge’s order.

Senator LEE. Okay. Let’s suppose that we have companies doing that, perhaps some, perhaps all. Perhaps they are doing it because they want to do it, or perhaps at some point, assuming Congress were to pass something requiring them to develop a back door, a universal key that could be used to unlock the encryption. If U.S. technology companies started doing that, perhaps some of them, perhaps most, perhaps all, that wouldn’t necessarily end the “Going Dark” problem, would it? Because wouldn’t we still have technology companies located outside the United States still manufacturing devices that wouldn’t be subject to that requirement or wouldn’t be subject to the same thing that would be convincing American companies to do that?

Director COMEY. I think that’s right, both—in two respects. Devices manufactured in other places might be different, and communications services from providers outside the United States might be different, which is what makes this such a hard problem. A big piece of it has to be international.

Senator LEE. Right. And so, even assuming Congress were to enact something requiring the use of a back door, the availability of a back door, a de-encryption key, if you will, it still would not solve the problem because there would be foreign manufacturers.

It also occurs to me that even assuming all U.S.-produced devices had a back-door key of sorts, it’s my understanding that it’s still possible to design an app that there are people all over this country and in other places throughout the world who can, with relative ease, design an application to be used on a smartphone, for instance, or perhaps on a computer that could provide encryption that couldn’t be unlocked through an encryption key made by the

manufacturer for the device in question. Is that your understanding?

Director COMEY. My understanding is, I think, the same, that with respect to a device, if the manufacturer were able to, as they were a year ago, to unlock on a judge's order the device, there may still be apps on the phone that are strongly encrypted, and so the content in that particular app would not be available once you unlock the phone.

Senator LEE. Correct. And so, if U.S. manufacturers were to start developing this back-door key and they used it, they had it, they made it available to law enforcement under appropriate circumstances, presumably those who were determined to go dark could and would start using an app that would itself not be subject to being opened by that same key.

Director COMEY. Yes, I hate to keep doing this to you. I struggle with that term, "back-door key." What I am talking about is a year ago the manufacturers of the leading phones in the United States could unlock them if a judge ordered it. I don't know whether it involved a key or their software. Somehow they are able to do that. But you are right, if we return to that world, there could still be—the sophisticated user could still figure out how to use something like TrueCrypt to protect other content on that device. I think there is no way we solve this entire problem. Encryption is always going to be available to the sophisticated user. The problem we face post-Snowden is it has moved from being available to the sophisticated bad guy to being the default, and so it's now affecting every criminal investigation that folks engage in.

But I agree; there is no way to solve this entire problem. I still think it's worth trying to solve a big chunk of it.

Senator LEE. And so, the big chunk of it here would involve U.S. manufacturers of U.S. diversity, notwithstanding the fact that we still would have the risk associated with apps that couldn't be opened by means of the same methods that you are describing.

Director COMEY. Sure, and there are other parts of it that would be difficult to solve, too. You mentioned the international aspect of it. Part of the solution, I hope, will involve an international set of norms somehow, because our partners in Europe very much face the same problem we do. And so, they are very interested in having the rule-of-law nations figure out so what should the rules of the road be with respect to encryption.

Senator LEE. Right. Okay. I see my time has expired. I do want to be clear. One of the reasons I asked the question is one thing that I think we ought to be cognizant of is that we ought not put U.S. manufacturers in a position in which they would be punished relative to other manufacturers, especially if U.S. manufacturers then saw a drop in sales because people, for whatever reason, preferred other products. And we ought to remember the limits on what we can do legislatively. If we were to mandate that legislatively, it would not necessarily fix the problem.

I see my time has expired, and I believe Senator Durbin is next in the batting lineup.

Senator DURBIN. Thank you very much, Senator Lee, and thank you, Director Comey, for being here.

I would like to speak to you for a moment about the gun issue and terrorism. I want to know if you believe that terrorist organizations around the world are aware of American gun laws.

Director COMEY. As I sit here, I don't—I assume that they are, and there is probably some specific I have been told that I can't remember sitting here, but I assume that they are.

Senator DURBIN. Let me just read a quote from one. An al-Qaeda spokesman, Adam Yahye Gadahn, American-born, who said in a 2011 video, and I quote, "America is absolutely awash with easily obtainable firearms. You can go down to a gun show at the local convention center and come away with a fully automatic assault rifle, without a background check, and most likely without having to show an identification card. So, what are you waiting for?"

That is what his quote was. Well, fully automatic weapons are not readily available for civilian use. Semiautomatic assault rifles are, and technology exists to convert them. There are reports that the San Bernardino shooters were trying to convert semiautomatic rifles into fully automatic versions. Can you comment on that?

Director COMEY. That is something we are looking at. There is an indication that they attempted to convert or did convert them successfully, and I can't give you the answer sitting right here.

Senator DURBIN. I guess the point I am trying to make for the record is that those who would do us harm know that it is easy to obtain firearms and weapons in the United States under our current set of laws.

I would like to ask you a question based on your opening statement, and I think I understood what you said, is that you have found a public—some type of utterance by the 2 killers that they were dedicated to jihad many years ago. And, I want to ask you whether that statement was made prior to the granting of a fiancé visa to the wife.

Director COMEY. Yes. And prior, frankly, to the rise of ISIL.

Senator DURBIN. And do you see any weakness in our system when it comes to visas or fiancé visas that that sort of information was not known to us before she was granted access to America?

Director COMEY. I don't know enough to say.

Senator DURBIN. We are discussing Visa Waiver Programs now and how we can change them to make them better. Roughly 60 million foreign visitors come to the United States each year. I understand 20 million are from the 38 countries where a visa is not necessary. And one of the things that is being discussed is to require a biometric examination or investigation before the visa waiver traveler boards the airplane. Do you have any thoughts on whether that would help to make us safer?

Director COMEY. I have not thought about it well enough to give you a reaction.

Senator DURBIN. I wish you would think about it, and I am sure you will. And it boils down to whether or not prior to having access to an airplane you present your fingerprints so that they can be checked against the information systems in Europe and in the United States.

Is there a good exchange of information, incidentally, between our European allies and the United States when it comes to such

things as the fingerprints of suspected terrorists and known criminals?

Director COMEY. It is good. It has gotten a lot better in the last 2 years, and there is still room to improve yet.

Senator DURBIN. I hope we can. I think it is very important. Let me ask you the question; I want to make sure it's clear in my mind. If someone on the No Fly List walks into a licensed firearm dealer in the United States, that in and of itself is not a prohibition against that person buying a firearm.

Director COMEY. Correct.

Senator DURBIN. So, even if that person is suspected to be a terrorist, they could purchase the firearm and leave with it, though your agents may then follow them or investigate them or keep an eye on them because of that purchase.

Director COMEY. That is correct. We have 3 days to review the background and so a hit, if someone walks in and they are on the No Fly List, we'll immediately be notified. We will have 3 days to figure out whether there is some prohibition under the law that allows us to stop the transaction. If not, they will walk out with a gun if the dealer transfers it.

Senator DURBIN. Absent some other disqualifier, the fact that they are on the No Fly List is not enough—a sufficient basis to deny the sale. Is that correct?

Director COMEY. That's correct. That's correct.

Senator DURBIN. I would like to bring this closer to home in terms of violence—gun violence in my State. We recently traced the crime guns that were seized in the most violent sections of Chicago, and we found that 40 percent of those crime guns were coming into Chicago from gun shows in northwest Indiana where there was no requirement for a background check before the sale was made.

Of course, it is not just firearms. It is ammunition as well, and we have ample evidence that those who are engaged in this gun violence make the short trip over the border into Indiana, secure their weaponry and their ammunition, and come back and kill people in Chicago.

What more can we do—we've brought up the issue, and I will not engage you on it because I think you know the debate about extending background checks to gun shows and internet sales. What more can we do with this knowledge, though, that these guns are crossing State borders into the city of Chicago and being used in the commission of crime?

Director COMEY. Well, under the current legal regime, we, but especially our colleagues at ATF, try to understand are there straw purchasers involved in that, are there gun show participants who know that they are selling to felons or prohibited persons, and try and make trafficking cases based on that. That's sort of the focus of trying to stop bad guys from getting guns at gun shows.

Senator DURBIN. Is there any surveillance of these gun shows to see if there are out-of-State license plates or anything of that nature?

Director COMEY. I think if there is a predicated investigation of a particular dealer within the gun show, there is appropriate surveillance. But I am not aware that there is surveillance generally of gun shows.

Senator DURBIN. Thank you. The last point I would like to make, in his opening statement our Chairman suggested that he would be open to the notion of prohibiting foreigners who are in the United States under the Visa Waiver Program to purchase firearms. That is a provision which I have been offering, and I would just say for the record I hope I could work with the Chairman and get his support in making sure that this loophole is closed. Thank you, Mr. Chairman.

Chairman GRASSLEY. On the Visa Waiver Program and guns, what I was trying to say is I want to go further than that.

Senator DURBIN. I will be glad to work with you.

Chairman GRASSLEY. Senator Flake.

Senator FLAKE. Thank you, Mr. Chairman. Thank you, Director Comey.

Encryption has been talked about some, but let me talk about some of the other vulnerabilities we have, and difficulties tracking information. I think we've discussed this maybe before, but the—the other ways for potential terrorists or terrorists to communicate here. It is obviously not just email, it is not just text messages. And I have asked some that are familiar with the field, if you had an event to communicate that you did not want anybody to follow it, how would you do it? And some say, well, you get on an app or a game, Words with Friends or some other game, and in the comment section there is a way to communicate within that. That is probably—I mean, there is no way to use encryption right now for that, but it is just in the realm of a lot of data, a lot of communication, a lot out there. Is that something that is concerning to the FBI? How—and what are we doing, without revealing sources and methods and everything else, to deal with that situation?

Director COMEY. Thank you, Senator. I don't want to say too much about it because I don't want the bad guys to get ideas they do not already have. But we have seen a number of cases in which subjects of investigations have communicated through gaming channels, either through more live action games or sometimes through app games on devices. Sometimes those do involve encryption, though. Those communications are encrypted in the gaming channel, which makes it as hard pressed to intercept with a court order as another encrypted channel. So, it's increasingly a feature of our work, I guess is what I will say.

Senator FLAKE. All right. Thank you. We have seen high-profile data breaches, obviously, with OMB. What is the FBI doing to ensure that we don't fall victim? A lot of information, obviously, held by the FBI is extremely sensitive. Are we taking the measures that we need to? And how can Congress help to ensure that that data is secure?

Director COMEY. Well, we worry about this every day, and we try not to be overconfident. I think we have very good systems, but we can't be satisfied, because as good as your system might be, if human beings have access to it, there is a vulnerability there. So, the FBI, especially since Snowden, has stepped up our game there to make sure we understand the potential insider threat. And so, we focus on it from a technological perspective and from a human vulnerability perspective an awful lot, is probably the best headline I can give you.

Senator FLAKE. You mentioned in your testimony that one of the areas of focus is to ensure that we deal with corruption at the border. Can you give us an idea of what you are doing to combat that?

Director COMEY. All of our field offices along the Mexican border have robust public corruption squads and efforts going on there, because anytime you have human beings in a role where there is potentially tremendous amounts of bad money, there's a risk of people being compromised. And so, it's worked all the way from the gulf over to the Pacific Ocean in California by all of our field offices. We work it in partnership with DHS because a lot of our focus is on is there corruption in the Border Patrol work force, for example, and I think we've built over the last couple years a pretty effective relationship there.

Senator FLAKE. Back to the visa situation, K1 visas have come under scrutiny now. You mentioned in previous testimony in the House the difficulty in vetting refugees, for example, because of lack of information about their background. I assume if that's true in Syria, it may be doubly true in South Sudan or in Somalia or elsewhere. And so, we have to rely heavily on interviews and assessments by field staff there.

What methods do we use there—lie detector tests—to try to vet whatever information is given? What do we have now? And what else can we do in that regard if there's a lack of information or data to check what they say against?

Director COMEY. State and DHS would be better qualified to answer this than I. I don't think they—in fact, I am quite confident they don't use a polygraph in that context. It's a problem. Where you don't have data that you can vet somebody against, you have to rely upon a skilled interviewer in a consular office or some other place to see if they can detect deception. And I know we have professionals doing it, but I don't know it well enough to tell you what particular tools they have considered using.

Senator FLAKE. You mentioned and, I think, we have all seen the professionalism of some of the State and local officials dealing with the situation, for example, in San Bernardino. That is not always the case elsewhere in the country where we have local officials who maybe need training or expertise. What is the FBI doing to ensure that our local partners are—are doing what they can to identify or to try to prevent or deal with these tragedies when they occur?

Director COMEY. With respect to terrorism attacks or—

Senator FLAKE. Yes, yes.

Director COMEY. Well, the bedrock of our effort is our Joint Terrorism Task Forces and the relationships we have also built with State Fusion Centers to make sure that we give our local partners what they crave, which is good information about what the threat is, how they might check it out, and good training on how to respond when there is an incident.

We have invested a tremendous amount of effort and money trying to make sure we equip State and local law enforcement to be able to respond well to these threats. We have just produced a video called "The Coming Storm," which is chilling but extraordinarily valuable, that through real-life movie actors shows how to respond to an attack in that case on a community college, the best way to organize yourself, the best way to respond. I have heard

great feedback from our State and local partners. We've made tens of thousands of copies of this. I think every university police force should have it. Anybody who is responsible for protecting a community should have it and look at it.

Senator FLAKE. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. First, thank you for having the hearing, to you and Senator Leahy. And, Director Comey, I am an admirer of yours—I was before you took this position and more so now—and an admirer of the men and women who work in the FBI. I think you do a great job. So, none of these questions are intended to impugn the hard work or integrity of all of you.

Look, we in New York, praise God, after 9/11 haven't had a successful terrorist incident. We have had a few in the country now. But it's because of the hard work of your folks and others on the Joint Task Forces that you mentioned, including the NYPD, who do a great job as well.

Here are my questions. In your testimony this morning, you told us the San Bernardino attackers were communicating online about jihad for some time so this raises two big questions which I would like to pursue. The first is, how come we did not know about these communications before the attacks? And the second is, how did she get a visa? How did somebody who is not an American citizen pass a visa test when they were communicating about jihad online before, no questions asked?

So, let us go to the first one. First, how do we know when terrorists are communicating online? And how does it sometimes get missed? How—I know you are exploring this, and I do not want to step on any ongoing investigations, but in general, this is going to cause great consternation to the American people and I think to every one of us, certainly me. Here we have somebody who is talking about jihad—two people—for a couple of years, and I always—you know, I think most Americans have the assumption that we're on top of things like this.

Director COMEY. And I can only answer it in general. I don't want to talk yet, if I could, Senator, about the particular case.

Senator SCHUMER. Okay. So, let's take a hypothetical. Okay? Someone is communicating—someone talking jihad over and over again online. Do we know of it in most cases? And what do we do about it?

Director COMEY. We will only know about it—if it's a private communication and not posting on a public forum or on a public facing social media site. If it's a private communication, whether it's electronic or it's by the mail, we are only going to know about it if we had some reason to believe that it was going on that allowed us to get permission from a judge to intercept those communications. That's where the community comes in. If folks tell us, "I think this guy is up to no good," then we can start to look at it and use our lawful tools. I know the Senators know this, but we don't monitor, and we should not in this country—

Senator SCHUMER. What about non-American citizens talking to American citizens?

Director COMEY. Well, again, that is governed by the rule of law in the United States, and so we have to have predication, the FBI or our intelligence agencies, to be able to intercept the communications of an American, whether they are communicating in the United States or overseas.

Senator SCHUMER. Okay. And in this case was there any public—okay. So, let me ask it more generally. Let's say there is some public posting, okay, on a Facebook page or something like that where either an American citizen or a non-American citizen communicating with an American citizen mentions jihad several times. Do we know about that? And what do we do about it?

Director COMEY. Often we know about it, either because a source of ours or an undercover of ours or a community member who sees it tells us about it, and then we can jump on it and use all of the tools that—

Senator SCHUMER. Do we have enough people monitoring these things so that when it is public, we know about it if no informant or no neighbor has told us?

Director COMEY. The answer is certainly not, given the size of the communication networks we're talking about. Millions and millions of people talking to each other and making Facebook posts and what-not, it's impossible to monitor—

Senator SCHUMER. But I would imagine on public postings you could get—we have computers, for instance, that stop child pornography with a certain image that's on there. Could we not get computers that spit out to us who publicly—and we don't know if these communications were public or private, and you haven't said, and I am not asking you to do that in this particular case. But could we not get a computer to spit out to us somebody who is talking about "jihad," "bombing"—you know, some words like this—repeatedly and to a variety of people?

Director COMEY. I want to be careful what I talk about in open setting, but there are tools, but they are limited in a way you would want them to be. But the United States Government, unlike some other governments in the world, does not monitor the internet.

Senator SCHUMER. So, a final question: Could we be doing more in these types of situations?

Director COMEY. We can always be doing more.

Senator SCHUMER. Okay. And is resources a problem?

Director COMEY. Resources is—I believe—

Senator SCHUMER. If we gave you unlimited money—you know, we're not going to do that, but we could give you considerably more. Would you be able, in more frequent cases, when publicly these things are mentioned, to be able to pursue them more thoroughly?

Director COMEY. "Maybe" is the answer.

Senator SCHUMER. Okay. Well, I'd like to get a classified briefing from you or others on the details of this because it concerns me.

Second, the Visa Waiver—the visa program, not visa waiver. So, let's just take a hypothetical. A non-American citizen has communicated online and used publicly, let's say—or now privately I guess we could intercept them, but it is hard—and used, you know, inflammatory words, language, intention, and they come here on a

visa, and let us even assume now it's not in a visa waiver country. How often do we catch them?

Director COMEY. I don't think I can answer that sitting here. I don't know enough about—I can't answer sitting here. I am sure we——

Senator SCHUMER. Don't you think we should know that?

Director COMEY. Well, I am sure somebody does. We could get you an answer in a pretty good way in terms of numbers.

Senator SCHUMER. Because after this hearing today, every American is going to be asking the question: How did this woman come in on a visa, a fiancé visa—I think it is called 1K or K1.

Director COMEY. K1, I think.

Senator SCHUMER. K1. If she was talking publicly—again, we will get into privately in the classified briefing—about jihad. Not this woman, sorry. How could a woman—strike “this” and use the word “a”—or man——

Senator FRANKEN. Hypothetical.

Senator SCHUMER. Hypothetical, right.

Director COMEY. And, again, assuming they are talking about it publicly.

Senator SCHUMER. Yes.

Director COMEY. On an internet forum or something?

Senator SCHUMER. Yes. Should it there—shouldn't that be somehow tied into our visa program?

Director COMEY. As part of the visa vetting process.

Senator SCHUMER. Yes.

Director COMEY. Yes. I can't give you a good answer sitting here, frankly.

Senator SCHUMER. No, but shouldn't it be?

Director COMEY. I don't know enough to say, because I don't know exactly what investment would have to be made to do that work and what would be the payoff on the other side.

Senator SCHUMER. Got it. Again, I will pursue this further with you both classified and nonclassified, and I thank you. My time is now up.

Chairman GRASSLEY. Senator Cornyn.

Senator CORNYN. Thank you. Thank you, Mr. Director.

If the FBI had a telephone number from a known foreign terrorist and there were people in the United States making phone calls to that known number, there are procedures in place through the NSA and other agencies to check against that known terrorist number to see if there're telephone calls by Americans to that number. Isn't that correct?

Director COMEY. Correct.

Senator CORNYN. And it doesn't involve any content at that point. Correct?

Director COMEY. Correct.

Senator CORNYN. Congress just voted and the President signed into law a piece of legislation that prohibits the National Security Agency from maintaining the bulk telephone records. Does that—does that development entail greater risk or otherwise limit the tools available to the FBI to be able to discover those sorts of communications?

Director COMEY. I don't know yet because the USA FREEDOM Act framework is sufficiently new that I can't give you a high-confidence answer on its effectiveness compared to what we used to have. In theory, it should work as well or better than what we used to have, but I don't know yet.

Senator CORNYN. So, it could entail more risk or no more risk?

Director COMEY. Correct.

Senator CORNYN. You can't say.

Director COMEY. It could—I just don't know at this point.

Senator CORNYN. Okay. I was shocked, as I bet a lot of other people were, particularly about your testimony with regard to encryption and its impact on the Garland shooting in my home State of Texas, 109 encrypted messages that still today the FBI cannot gain access to. Is that correct?

Director COMEY. Correct.

Senator CORNYN. And the only way you would be able to gain access to that, again, is not because you are monitoring private messages. It would be you would go to court and show cause, meet the legal standard in order to get a court order to then give you access to those records.

Director COMEY. Correct.

Senator CORNYN. And you said there are telecommunications—there are phone companies or, I should say, manufacturers who are marketing their encryption as a way to gain market share in America, to advertise that these are private conversations that not even courts can order access to.

Director COMEY. I think there are device manufacturers who include that in their description of why their products should be used.

Senator CORNYN. And you said encryption is part of terrorist tradecraft. Correct?

Director COMEY. That's for sure.

Senator CORNYN. To me that is a staggering situation because it still persists today. Correct?

Director COMEY. Oh, yes, and growing.

Senator CORNYN. And so, while we are all horrified and repelled by what we saw in San Bernardino and what we saw in Paris, there could well be similar communications, not in those cases but in other cases, going on today and the FBI would not be able to gain access to those communications between terrorists even with a court order.

Director COMEY. That's correct. And strongly encrypted, end-to-end encrypted, even if a judge issues an order, if we intercept it, it is still encrypted and unreadable.

Senator CORNYN. Do you consider that a danger to the American people? Does that increase the risk of terrorist attacks that could go undetected before the carnage occurs?

Director COMEY. I do, which is why we've been talking about for the last 2 years so much.

Senator CORNYN. Well, I appreciate very much your making this important point, but it concerns me a lot that Congress has not acted to do anything to give you the tools that you need. I appreciate the way you have tried to discuss this with the various manufacturers and other entities involved, but it strikes me is if they are

gaining market share by advertising their encryption and saying that not even the Federal Government in a terrorist investigation can gain access to it, that is a real problem. And so, I think you said you hoped to get to a place where the companies can comply with a court order, but do you think it would be useful for Congress to actually try to do something about this? Or should we just wait for the voluntary compliance by the industry?

Director COMEY. I think it would be useful, as Congress has done, for Congress to try to drive this conversation, to ask to draw people into it to figure out what we can do, because I do not want to hurt American business, but I also have a responsibility to try and protect the American people. And all of us care about the same thing, so I appreciate Congress trying to drive this conversation.

Senator CORNYN. Well, I think your testimony here today will help do that. I think it has surprised and shocked a lot of people.

I want to just close on this line of questioning, Director Comey. We are at a point in our Nation's history where the public doesn't trust Government. I think a Pew poll indicated less than 20 percent of Americans say they trust their Government most of the time. And, unfortunately, many Americans have lost faith in our national institutions, including our justice system, and I know how much you care about that and how much you've dedicated your life to making sure that people can trust law enforcement and our justice system. That faith is endangered when attempts are made to pervert it in favor of the powerful who would like to create different rules for those who rule.

I know this is a sensitive matter, and I'm not going to ask you about the content, but I know the FBI is currently investigating the private email server of the former Secretary of State, and it has troubled me, and I know others, when some people have attempted to disparage or otherwise predict the outcome of the ongoing FBI investigation. I know the President himself said that we don't get an impression that there was purposely efforts to hide something or to squirrel away information. Does the President get briefings on ongoing investigations by the FBI like this?

Director COMEY. No.

Senator CORNYN. So, he would have no way of knowing what the status of the FBI investigation is?

Director COMEY. Certainly not from briefings from the FBI.

Senator CORNYN. I know a former senior official at the FBI and the current president of the Law Enforcement Legal Defense Fund told the New York Times that injecting politics into what is supposed to be a fact-finding inquiry leaves a foul taste in the FBI's mouth and makes them fear that, no matter what they find, the Justice Department will take the President's signal and will not bring a case. But I just want to ask you to perhaps repeat something you said earlier when you said that people at the FBI, including you, don't give a rip about politics. Is that your position?

Director COMEY. That is true through and through the FBI.

Senator CORNYN. So, for politicians of whatever level, whether it's the President of the United States or Members of Congress or anybody else, trying to lobby or intimidate or influence an investigation by the FBI, that does not work, at least under your leadership.

Director COMEY. It does not matter—I don’t want to hurt anybody’s feelings, but it doesn’t matter what anybody thinks or feels about our work. We are competent, we are honest, and we are independent. We are going to do our work the right way, and we care only about the facts. That’s who we are.

Senator CORNYN. Well, that is certainly consistent with the way you have conducted yourself, I think, in your public life, and I think that will help restore in some small part people’s confidence that there are people trying to do the right thing for the right reasons. So, thank you very much.

Director COMEY. Thank you, Senator.

Chairman GRASSLEY. Senator Klobuchar.

Senator KLOBUCHAR. Well, thank you very much, Mr. Chairman, and thank you, Director Comey, for being here. I really appreciate it.

One of the things that we haven’t gone into as much is the online recruiting of terrorists. Minnesota, as you know, has been very aggressive—our FBI and our local law enforcement, our U.S. Attorney Andy Luger—in going after cases of people who have been recruited, much of it online—not all of it, but much of it—to join ISIS or, before that, al-Shabaab. And I have seen these recruiting techniques myself. Your agents have shown them to me. And I wondered what is being done about that. And, you know, it may have played a role—I know the investigation is still going on into the tragic shooting in San Bernardino, but what is this emerging threat? What can be done? There has been discussion about getting the companies to take down these sites as much as possible. Just talk a little bit about that.

Director COMEY. Thank you, Senator. ISIL tries to crowdsource terrorism. They obviously, as we talked about, aspire to send operatives here. We as a country have made that very, very hard, although it is something we focus on a lot. And so, they also try to inspire people to kill on their behalf. They send a message in a very slick way that resonates with troubled souls, with people who are unmoored and seeking meaning in their life, kids a lot of times, or older people who have struggled in some way. And it is a very, very seductive message that, by virtue of its quality and its quantity, has a huge impact on the troubled mind because it is buzzing all day long that these people can consume this. And their goal is to draw folks into this closed circle online where they are constantly bombarded with, “This is the way to meaning, this is the way to meaning,” and that shapes a troubled mind.

And so, what we try to do is make sure we are aggressively investigating that to find those that are on that path consuming and potentially radicalizing, and then work with a whole lot of other folks to try to help kids who might be vulnerable to it, and not just to their poisonous message but to all kinds of poisonous messages that inspire people—inspire people to violence.

So, we are about to come out with something called, “Don’t be a puppet,” which is—I am no judge of what is cool, but I am told this is cool—almost like an online game for schools to have kids learn this is the way they come after you and here is how you resist it, whether it is al-Shabaab or ISIL or some domestic extremist group. Those are the two ways we try to attack it.

Senator KLOBUCHAR. Very good. And as you know, we have one of the sort of pilot projects, the Countering Violent Extremism group, and it has been used with our Muslim community, which we are very proud of in Minnesota, has been working to try to prevent these kids from getting involved in this in the first place. And I really appreciate the work that you are doing. I just encourage you to do more. We need more funding. We are hoping we can get some out of this budget for these projects to fight Islamic extremism. So, thank you for that.

I know that Senator Flake asked you about cooperation with local law enforcement, and I heard you bring it up in your initial statement. Do you think they have enough resources to deal with what we are—Senator Murkowski and I are introducing the COPS bill again to try to increase funding there, but could you talk about that?

Director COMEY. Our State and local partners are strapped across the country coming out of the painful cuts they have endured over the last 8 years, and so they are still contributing their stars to our task forces, but I know what it costs them because they are shorthanded across the country.

I travel to our field offices. I have been to all of them once. Now, I am almost halfway through the second time. Every visit I talk to State and locals, and I hear this over and over again. They are being asked to do more and more with less. They are trying to become better at community policing. That is very hard when you are having to have officers cover twice the territory they used to cover. They don't have time to get out of their cars and meet people. So, it is a constant theme I hear from our partners.

Senator KLOBUCHAR. Thank you. And I wanted to end—a lot of my colleagues have you asked you about encryption, and I know you were here before and talked about efforts to try to work with the phone companies. I thought your testimony was very interesting today when you talked about the fact that some of suspect that it may not really be a technological issue as much as it is a business model issue. But—so, if that is all the case, what has been done to improve it since that time? Has there really been changes except for discussions with the phone companies? You said in answer to one of the questions that a good chunk of it could be resolved. How would we resolve that? Is it just simply the international norms you talked about where you would have agreement between countries to when—that our court orders and their court orders could be followed? I am just trying to get to a solution here as soon as possible. I just keep waiting for the next ticking time bomb of something where, you know, our law enforcement is not able to access it. And you know it is domestic as well. It is not just terrorism investigations. Cy Vance has made this a crusade, going around talking about the problem in gang cases and some of the others. And I just remember as a prosecutor sitting in on wiretaps, seeing that kind of information. These are the old days when people were using landlines and when there were less sophisticated cell phones, and it was a major part of our investigations.

Director COMEY. I think a big part of the problem can be solved if folks who are currently producing and selling devices that can't be unlocked by judges' orders or communications that can't be

intercepted by judges' orders were to change their business model in this respect—not to give us a key. I don't want a key. I don't want to tell them how to do their business. But figure out how they could change their model so they comply with judges' orders.

As I said in my testimony, I actually don't think that is a technical problem. The folks making the phones today, they were doing that a year ago, and nobody said their devices were insecure so we ought not to buy them. And so, I am hopeful—I mean, I am an optimist. I am hopeful that people, now that they understand how big the threat is, will consider those changes and get us to a place so we can address a big chunk of it that way. It's not going to solve the entire problem, and I agree very much that you don't want to just chase the problem offshore, and so there does have to be an international component to this. But a big start would be people acknowledging it is actually not a technical problem; we have chosen to operate our business this, for good reasons; but we should stop saying you are going to break the internet if you ask us to do this, or the Director of the FBI wants to stockpile keys. No, I don't. I don't want the key to anybody's house. You should figure out—when a judge says there is something in your house that this Nation needs to be safe, you figure out how to come out of the house, use a window, use a door, use a slot, whatever keeps your house safe. We should not tell you how to do it, but we should get to a place so when a judge says this is necessary, you are able to comply.

Senator KLOBUCHAR. And you are talking here about court orders, and you are talking here about an international norm, given that the world has united against ISIL and this kind of other terrorist evil. So, some way that we can find international agreement on when this information is given to pursue these very important investigations.

Director COMEY. Yes, I think reasonable people have said that is a part—that should be a part of it, and I think they are right.

Senator KLOBUCHAR. Thank you very much.

Senator HATCH [presiding]. Thank you, Senator Klobuchar.

Mr. Director, we are really happy to have you here today, and I want to personally express my gratitude for the work that you are doing, the work you have done in the past, and for the good way you approach law enforcement in this country. You are doing a great job.

Last week's tragedy in San Bernardino was the worst terrorist attack on American soil since 9/11. Now, the shooters claimed allegiance to ISIS, and ISIS has called them its followers. I think it's important to call this attack what it is. Do you agree with me that this was an act of terrorism?

Director COMEY. Yes.

Senator HATCH. Do you agree that it appears this terrorist attack was at least inspired by ISIS?

Director COMEY. We are still sorting that out, Senator. It was definitely claimed by the killers at or about the time of the killing that they were doing this on behalf of ISIL, and ISIL then has embraced them as followers. There's more work to be done to understand the motivations more clearly.

Senator HATCH. It would seem hard to not say that ISIS had something to do with it.

Director COMEY. Right, ISIL inspiration may well have been part of this.

Senator HATCH. Sure.

Director COMEY. But these two killers were starting to radicalize toward martyrdom and jihad as early as 2013.

Senator HATCH. I agree.

Director COMEY. And so that's really before ISIL became the global jihad leader that it is.

Senator HATCH. Within 24 hours of this terrorist attack, the Attorney General stated that her, quote, "greatest fear," unquote, was the possibility that it could lead to anti-Muslim rhetoric. And after 130 deaths by ISIS in Paris and 14 dead Americans last week, my greatest fear is not rhetoric. I mean, in all honesty, my greatest fear is more attacks and more dead Americans.

If we were to put it this way, what would be your greatest fear after last weeks' terrorist attack?

Director COMEY. My fear, which is not new—it has been a feature of my work since I started this job—is what don't we know, what can't we see, and that is the particular challenge of those radicalizing online, consuming propaganda, and trying to stay beneath our radar. This confirms to us what we have said all along, as have many other cases. The reason we have cases in all 50 States is a very real concern that people are radicalizing in a way that is hard to see. That inability to see is my biggest worry.

Senator HATCH. Well, I share that.

Let me just say this—and I would like to follow-up on Senator Lee's line of questions regarding the so-called dark problem. I have two questions.

First, with respect to control of encrypted data, U.S. tech companies do not want to be the middleman between law enforcement and technology customers. How do you—how do you reconcile this concern with the needs of law enforcement? And have you considered alternatives that would meet the needs of law enforcement but not put the United States tech companies in the awkward position of middleman?

Director COMEY. I'm not sure I know exactly what they mean by middlemen. I don't want anybody to be the middleman for law enforcement. But everybody in the United States has, I believe, an obligation to endeavor to comply with judicial orders in criminal investigations, whether you are a bank or you run a sandwich shop or you run a technology company. And so, I don't want anyone to be the middleman, but I want everyone to be in a position to comply with judges' orders. That's what the rule of law is about.

Senator HATCH. Thank you. Second, U.S. tech companies are not the only businesses that offer encryption to countries—to customers. Businesses in other countries offer it as well. Now, if we require U.S. tech companies to provide decryption keys, won't users simply look to technologies from other non-U.S. companies to conduct their activities? How do you respond to that concern?

Director COMEY. That's a serious concern. First of all, I do not want anyone to supply encryption keys, but if we went to a place where American companies were required to figure out a way to

comply with judicial orders, they do make a serious argument that what that would do is chase our business overseas. I'm not in a position to evaluate that argument. A little part of me is skeptical that people would stop buying the great phones we make in this country because a judge might order access to it. But I am not really an expert on that.

So, I do think a part of this has to be an international compact of some sort. None of us want to hurt American business. But at the same time, there are costs to being an American business. You cannot pollute, you cannot employ children. There are certain things we've decided as a country we want to govern ourselves this way. And so, in a way, I think we have to figure out what's right for America first, and then try and figure out how to reduce the harm that might come competitively.

Senator HATCH. Okay. I would like to turn now to the issue of rapid DNA. Last week I introduced bipartisan legislation with Senators Feinstein, Lee, and Gillibrand to update our Nation's laws to take account of this exciting new technology. Now, rapid DNA devices are self-contained. They are fully automated instruments that can be placed in booking stations and that can both develop a DNA profile from a cheek swab and compare the results against existing profiles in less than 2 hours.

Now, my bill, the Rapid DNA Act of 2015, would allow law enforcement officials using FBI-approved rapid DNA instruments to upload profiles generated by such devices to the FBI's Combined DNA Index System and perform data base comparisons.

Director COMEY, you have spoken in the past about rapid DNA and how this technology will help law enforcement. Do you believe that rapid DNA technology is important? How will it impact law enforcement? And do you believe Congress should pass legislation authorizing its use within standards and guidelines promulgated by your agency?

Director COMEY. That authority that's in your bill would help us change the world in a very, very exciting way. That would allow us in booking stations around the country, if someone is arrested, to know instantly or near instantly whether that person is the rapist who has been on the loose in a particular community before they are released on bail and get away, or to clear somebody, to show that they are not the person.

It is very, very exciting. We are very grateful that we are going to have the statutory authorization, if that passes, to connect the rapid DNA technology to the national DNA data base.

Senator HATCH. Well, thank you. My bill, the Rapid DNA Act, will not affect when or under what circumstances law enforcement collects DNA samples. These decisions would be governed by State or other Federal law. What it will do is affect where samples are processed and how quickly they are processed.

Now, Mr. Director, what would you say to individuals who may be concerned that rapid DNA technology will raise privacy concerns? And what would you say to individuals who may be concerned that this technology could affect the integrity of the FBI's Combined DNA Index System, or CODIS? And I would note that my bill restricts access to CODIS to FBI-approved rapid DNA in-

struments operated in accordance with FBI-issued standards and procedures.

Director COMEY. First, you said it well, Senator. Folks need to understand this is not about collecting DNA from more people. It is about the DNA that is collected when someone is arrested, being able to be analyzed much more quickly, that can show us in some cases this is the wrong person or can show us in some cases this is someone we have to be very worried about. That is good for our justice system as a whole.

And you are exactly right. The national data base, the CODIS data base, is the gold standard. This legislation does not make it any—water down the standards that are applied before a DNA result can be pressed against that data base. We're still going to have high standards. We're still going to require that this is the gold standard for identification in the United States.

Senator HATCH. Well, thank you, sir. Senator Franken is next.

Senator FRANKEN. Thank you, Mr. Chairman.

Director Comey, first I would like to thank you for appearing today. It's good to see you again, and you do a great job, I think as all the Members of this Committee agree.

Before I turn to my questions, I want to extend my thanks to the Bureau and to you and to your agents for assisting in the Federal civil rights investigation surrounding the death of Jamar Clark in Minneapolis. I supported the decision of Mayor Hodges and Police Chief Harteau to call for an independent investigation. In my view, a full, thorough, and transparent accounting of the facts is necessary to get to the bottom of what happened in that tragic event and to restore trust between the North Side community and the police and law enforcement. So, I want to commend the FBI agents involved for their professionalism and for their commitment to seeking justice.

I wanted to just—a lot of things have been discussed in this Committee, including the “Going Dark,” the encryption issue, and I just want to make sure that I have clarity on this and maybe help other people clarify it for them.

Basically, tell me if I heard you right, that a terrorist in the United States could—that there is—is there a distinction between—there are two distinct but related concerns that law enforcement has about encryption concerning information sought by law enforcement is on an encrypted device—we are talking about the phone—and the concern that encrypted—that the information might exist within an encrypted app on that phone. And so, some of these apps are available freely online and add an extra layer of encryption.

Can you speak to the Bureau's concerns related to these issues? You're basically saying that there sort of are two layers, and if you get rid of the first layer, you'll have more—I mean, you'll obviously be—it will be a great deal more people that won't be caught up or that won't have that encryption? Is that what you are saying?

Director COMEY. I think what has changed—encryption has always been available, always been available to the sophisticated user, “always” meaning for decades. What changed over the last 2 years is encryption went from available to being the default, and so now, with some of the leading phones in the United States, that

phone is encrypted by default. So, if we recover it at a crime scene, with a judge's search warrant order we cannot open it. It has been designed that way.

Senator FRANKEN. And I know you are not asking for a key. You are asking for the company to be able to follow the judge's order.

Director COMEY. Right, which they could do—2 years ago they could do it and did it routinely, and I think their devices were still considered pretty secure. But you're exactly right. There may still be within that device, especially for sophisticated users, other encryption tools that are on particular apps, or there is actually something too complicated—

Senator FRANKEN. Can we get some data on this? I mean—the last time we looked at this, this Committee looked at this, we had Deputy Attorney General Yates, and I asked her for more information about the scope of law enforcement's concern, because I know there's a lot of this is about just normal crime and not about terrorism. And I think what you're suggesting is that a terrorist might be able to get that app, that's why—that foreign app, and that's why we need an international agreement on this. Right?

Director COMEY. Yes, you are exactly right. This is mostly a local law enforcement issue. But we are gathering the data that you asked for, and I'll have to get back to you on exactly when we are going to get it to you.

Senator FRANKEN. And I know that you have mentioned it.

Director COMEY. Yes.

Senator FRANKEN. Okay. I want to make sure I am clear on something else from this testimony. I'm just sort of reviewing the whole day for myself. I understand if someone on a terrorist—terrorist watchlist tries to buy a gun through a licensed dealer, the FBI is alerted.

Director COMEY. Correct.

Senator FRANKEN. And it can delay the sale for 3 days?

Director COMEY. Under the law, we are allowed up to 3 days.

Senator FRANKEN. So, okay. But ultimately do you have legal authority to deny the sale?

Director COMEY. Not unless there is another prohibitor under the law, felon or mental defective—

Senator FRANKEN. Well, at least you have that 3 days.

Director COMEY. Yes.

Senator FRANKEN. If someone on a terrorist watchlist—this is someone on a terrorist watchlist. In 3 days, if there is no other indicator, they can get their gun. That to me is a problem.

Now, if someone on a terrorist watchlist tries to buy a gun online or at a gun show, no one is legally required to notify the FBI.

Director COMEY. I believe that is correct, yes.

Senator FRANKEN. Okay, so I have that correct.

So, to fix this, if we're talking about keeping guns out of the hands of terrorists, and presumably people on the No Watch List are there for a reason, or maybe there is a false positive, but it would seem to me that we would have to be doing both. Having—if we are really interested in keeping guns from terrorists, we would have to enforce both—say you can't sell a gun to someone—or there has to be 3 days or some kind of look at that person, and also the gun—the gun sale, the sale at a gun show, the gun show

loophole would have to be solved, too. I mean, in other words, if we're worried about guns falling into the hands of people on terrorist watchlists, we also have to close up the gun show loophole as well as cleaning up this loophole, which is the terrorist watch loophole. In other words, this is a reason to do both in—let me put it this way—you don't have to answer. This is the reason to do both.

Okay. Thank you.

Chairman GRASSLEY. Senator Perdue.

Senator PERDUE. Thank you, Mr. Chairman.

Director, we are lucky to have you. Thank you for the sacrifice you make in doing what you do. I'm glad you are on the wall.

I would like to go back and clear up just to make sure I understood the testimony today as well. I applaud the FBI for being the first to call this an act of terrorism—not that I want it to be an act of terrorism, of course, but you guys looked at the facts and said the American public needs to know the facts. Thank you for that.

But I am a little confused. An act of terrorism, I haven't heard today it connected directly to ISIS. At this point, I know in this environment you may not be able to talk about that, and if not, that is fine. Can you talk about that? Do we have evidence that this was directly connected to ISIS influence in the U.S.?

Director COMEY. There is some indication that they were at least, in part, inspired by ISIL, so yes. We're trying to sort out what other contributions might there have been to their motivation, and we may never fully sort it out because human motivation is hard. But at least, in part, we see an ISIL inspiration.

Senator PERDUE. And you may not want to comment on this either, and I apologize for asking these direct questions. But in the past, just for the American people and for Congress, the FBI has been a stalwart in helping to protect the American people over time. In the past and on your watch, are you aware of planned attempts that have actually been preempted by the FBI that we may never know about.

Director COMEY. Yes, many.

Senator PERDUE. Okay. Thank you.

In speaking to the increase in the latest spate of ISIS attacks, is their planning getting better? Are their tactics getting better? Are there networks expanding? I know that the Malik and Farook team bought their weapons through a neighbor. My question is, is there a network issue here? And are the networks growing in the U.S.?

Director COMEY. We are looking at, obviously, in San Bernardino to see was there anybody else involved in assisting them, and so separate from San Bernardino, we have not seen this, we have not seen ISIL cells or networks in the United States. So far as we can tell, they have not succeeded in penetrating our borders with their operatives. That's an aspiration of theirs. We have got to worry about it all day every day. But, instead, what they're doing is motivating individuals or very, very small groups of people to commit murder on their behalf. That is the crowdsourcing phenomenon we have been dealing with.

Senator PERDUE. Thank you.

Can you confirm that ISIS adherents have attempted to gain access through the refugee—refugee resettlement program? Do we actually have cases where through the resettlement—I think there are 2,200 people or so that have come in so far, and we're trying to bring another 10,000 in the first phase of this. Have we actually had cases where we have identified ISIS adherents in that first group?

Director COMEY. Not to my knowledge.

Senator PERDUE. Are you aware that Canada is increasing their Syrian refugee acceptance rate from less than 5,000 to over 25,000, the latest number I saw? And with the border that we have with Canada—we don't talk about that border much—is the FBI aware of that, or are they paying attention to that relative to what we need to do? To me that vetting in Canada—and Canada is just as important as our own vetting here with our K1 and our Visa Waiver Program.

Director COMEY. And they get that. The head of the RCMP is a friend and colleague of mine. He called me to tell me that their government had made that decision and to explain and to encourage us to work together to vet those people.

Senator PERDUE. And what changes would you like to see in the K1—with Malik, was she actually given an interview in the K1 process, do you know? Or do we know that?

Director COMEY. I do not know well enough to say at this point.

Senator PERDUE. Okay.

Director COMEY. I know the process requires it. We are still trying to fully understand exactly all of her contacts.

Senator PERDUE. Are there changes you would like to see, the FBI would like to see in the K1 program or in the Visa Waiver Program?

Director COMEY. I don't know enough yet to say as a result of this case.

Senator PERDUE. Okay. And the last thing, very quickly, in the Trans-Pacific Partnership there is language in there that would prevent national laws being implemented in countries that would require manufacturers to provide access to products' encryption technologies. Some critics think that that would limit our own ability to provide legislation that would give you a solution to the potential "Go Dark" solution. Does the FBI have a point of view on that yet?

Director COMEY. We don't.

Senator PERDUE. Okay. Thank you, Mr. Chairman. Thank you, Director.

Chairman GRASSLEY. Next is Senator Blumenthal and then Senator Coons, and if you can stand me for 7 more minutes, I have a second round of questions.

Senator BLUMENTHAL. Thanks, Mr. Chairman, and thank you, Director Comey, for your excellent work and your great service to our country. Thank you to your family and most especially to your wife, Patrice, who has done so much for the children of Connecticut and now for others around our country. I have just come from—

Chairman GRASSLEY. She is from Iowa, too.

Senator BLUMENTHAL. Thank you, Mr. Chairman, for that correction.

[Laughter.]

I have just come from a hearing at the Armed Services Committee where Secretary Carter was testifying, and I want to first make the point that we often thank our men and women in uniform, which I do readily and repeatedly, and I do again now. But I also want to thank the very brave men and women who work under your command, who enforce our laws and help to keep us safe, along with all of our law enforcement men and women around the country, police at every level, and are in a sense also at war.

In fact, Secretary Carter said, and I'm quoting, talking about ISIL, "The reality is we are at war. That's how our troops feel about it because they are taking the fight to ISIL every day, applying the might of the finest fighting force the world has ever known."

Do you feel that we are at war also within our borders against forces of terror that are linked to those forces abroad that our men and women in uniform are fighting?

Director COMEY. Very much, Senator, and our people feel that passionately. Our people are tired, and we are working very, very hard. They're working very, very hard. But what motivates them is these people want to kill our people, and we are at war with these people. And so, stopping them is what—is the reason we do this work.

Senator BLUMENTHAL. And the President well identified this new phase that perhaps is an old phase in larger scale, the phase of ISIL and ISIS reaching outside the theaters where they have fought so far, reaching into this country. You have referred to crowdsourcing as the San Bernardino experience, and outsourcing that threat to new recruits, to homegrown radicals, may be part of the threat here. But you would agree that we face a war every bit as dire and dangerous here at home as we do abroad.

Director COMEY. Yes. The threat obviously and the density of these savages is less here in the United States, but the nature of it is very similar.

Senator BLUMENTHAL. And I know that you've responded about the importance of cooperation in terms of information and other kinds of assistance that is provided by members of the Muslim community, just as cooperation and support is essential from nations that have a majority of Muslims abroad in our fight against ISIS and ISIL. They are our natural allies and friends and partners in this fight against extremist terrorism and violence abroad. And I want to ask you about some of the statements that are made about closing borders and about religious tests at our borders, other kinds of religious tests that, in my view, are unconstitutional, but also strike me as unwise because we need that cooperation.

Are the statements themselves potentially inhibiting that kind of cooperation and support and help that we need?

Director COMEY. Thank you, Senator. I don't want to comment on anybody's statements, but I can make, I think, the point that you are interested in. ISIL is trying to recruit—recruit in Muslim communities. They are trying to motivate people who may be of the Muslim faith who are unmoored in some way to become part of their poisonous endeavor. The people who so often tell us about people like that are other Muslims who help us, and so we've

worked so hard over the last 15 years to build relationships of trust that allow us to find out who might be trouble and to stop it. That's in everybody's interest. And anything that gets in the way, that erodes that relationship of trust, is not a good thing.

Senator BLUMENTHAL. And Muslims who live in our Nation are fellow Americans, many of them, equally interested in preventing threats and violence, as any one of any religion.

Director COMEY. Our experience, they are—what is wonderful about this country is we are incredibly diverse. They are part of that diverse polyglot, and they love our country, which is why they help us when there is a killer in their midst or someone on the path to being a killer in their midst. We have to continue this. As I said at the beginning, we are all in this together. We need each other.

Senator BLUMENTHAL. I applaud your very clear and emphatic, unequivocal statement about that point.

I want to shift to another terrorist act, at least one that strikes terror, not of the same motivation but involving the apparent racist-motivated violence in Charleston. The FBI background system known as NICS was applied in the case of Dylann Roof's purchase, but only too late to prevent him from buying a gun. The 72-hour loophole that I have tried to close enabled him to walk away with a gun that he sought to purchase. Thanks to that loophole, after the 72-hour period, since the background check was not completed but would have precluded him from buying a gun, he was enabled to have that firearm. Gun retailers have sold 15,729 guns in the last 5 years to individuals who were not legally allowed to purchase them, and about 5 months ago, I think, you commissioned a study that was to last 30 days to examine how Dylann Roof was able to buy that gun. I think that report would help us in Congress to understand what went wrong and how to fix it, and most especially, if the 72-hour loophole enabled him to buy that gun, as appears to be from the facts that we have been told so far, the report would be very helpful.

So, my question is: Can you update us as to the status of that report?

Director COMEY. Certainly, Senator, and we would be happy to get you a detailed briefing on it, because the work was done, as I asked, in 30 days, and it did two things: It confirmed the facts as we understood them close to the murders in Charleston, that there was a mistake made by our processing clerks that was compounded by a mistake in the records of the South Carolina jurisdiction where he would have been—where the prohibitor came from. And so that confirmed what we knew. What it most importantly told us is how can we get better.

The law is what the law is. We have 3 days to process these thousands and thousands and thousands of them, and so we are working on a number of things to get better: one, to improve the records that are put in by State and locals, to improve our technology, and to surge resources. The number of gun purchases continues to climb. It has climbed dramatically in the last week. We have got to make sure we have enough folks—if all we have is 3 days, we have got to make sure we have enough folks to do that. And so, those are the three buckets: better records, better tech-

nology, and more importantly, more human beings on the phones to process them more quickly.

Senator BLUMENTHAL. So, resources are really important, resources in technology, resources in people, and resources in records that you depend on because many of them come from State and local authorities as well.

Director COMEY. Correct.

Senator BLUMENTHAL. My time has expired. This whole area is tremendously important. I want to thank you for being here today, and just to clarify, racial and religious supremacists often use terrorist-type tactics, even though we would not call them “terrorists” today. But I appreciate the attention that you are giving to the potentially white supremacist-motivated acts of violence in that church in Charleston. Thank you.

Chairman GRASSLEY. Senator Coons.

Senator COONS. Thank you, Chairman Grassley, and thank you, Director Comey, for your service and for your testimony before this Committee today.

I was very pleased to see in your testimony before the Committee a focus on the Violence Reduction Network, a Department of Justice initiative that is truly helping a group of now ten smaller cities, like my home town of Wilmington, Delaware, that have seen a dramatic rise in violent crime and in homicides. We are, sadly, on track for a record year of shootings and homicides, and I am grateful for your focus and for the FBI’s focus on providing technical and investigatory resources to help State and local law enforcement deal with this rise in violent crime in a few cities and to learn from the policing examples of other communities and Federal agencies that have real knowledge about how to better deploy investigatory resources.

So, tell me, if you would, how we can better support valuable programs like the VRN and how, in your view, it’s been most effective in connecting FBI resources to cities like Wilmington, Delaware.

Director COMEY. I will start with the effectiveness point first. I think what makes it special is we bring together in a place like Wilmington everybody who cares about this issue or might have a specialty that is useful, and where I think we can bring a lot to bear is our understanding of technology and our analytic resources so that we help a local jurisdiction understand what is the pattern, what is the trend, and what are the pieces of information that we can lawfully gather that would be useful to you in focusing on, because it is almost always small groups of predators, finding them and ripping them out of the community. And that is a—it’s not rocket science, but it often brings rocket science—rocket scientists to the fight in a really important way.

I think the way you can support it is, as you just did, talking about its value and making sure that appropriators and others understand that when the Department talks about this, it is making a difference.

Senator COONS. Thank you. I am an appropriator on the relevant Subcommittee and have advocated for it with the head of OMB and the Attorney General, but would be grateful for any other advice or insight you would care to offer about how we can sustain it,

make it more effective. Certainly, the work to reduce violent crime is far from over in my home town and in the 9 other cities around the country, and I am hopeful we will sustain this program until we see some significant reduction in violent crime.

I would like to mention another issue, if I could, about cybersecurity. The Senate recently passed the Cybersecurity Sharing Information Act which permits DHS to scrub personally identifying information it receives from private entities, but only after it secures the approval of a number of agency heads, including yourself in your role as Director of the FBI.

Have you had any communications with other agencies yet about how this process will work? And are you committed to ensuring that DHS can actually conduct a robust scrubbing of personally identifying information?

Director COMEY. I haven't had any conversations about that, but the second part is easy. We'll do everything possible to make sure that it works and works the way Congress designed it.

Senator COONS. Well, thank you. I would urge you to engage in those conversations. I think this process is going to move relatively quickly, or so I hope.

In October, President Obama secured from President Xi of China a striking landmark admission that China had been engaged in economic espionage, cyber attacks—that is something you have testified about here before—and a commitment that those attacks would end. Yet press reports suggest that literally a day after President Xi's visit, Chinese cyber attacks resumed.

Has the FBI detected any change in Chinese cyber espionage behavior following President Xi's promise? And what do you recommend in terms of action by the Senate to try and address this ongoing challenge to our Nation's innovation and inventions?

Director COMEY. It's too early to say. We're watching it very, very carefully. Given the long-tail nature of Chinese cyber espionage and theft, even if—I'm not sure that I would expect a change, even if one was going to happen, that would be visible yet. And so, we are watching the space very carefully. We have had good conversations with our Chinese counterparts. I have told them I do not mean to be rude, but the FBI Director is paid to be skeptical. I am deeply skeptical. And so, we will have to watch and see what the facts show us, but I cannot say yet.

Senator COONS. I think it is deeply disturbing and hostile behavior that we need to continue to be engaged. I have heard from far too many American companies that they have lost vital both economic secrets and from some Federal agencies that they've lost vital national security secrets, and I appreciate your hard work on this.

Last, I am the Ranking Member of the Oversight Subcommittee, and last month we held a hearing at which DeKalb County Police Chief Cedric Alexander, who is himself a 30-year law enforcement veteran, testified that the notion that there is a so-called Ferguson effect is of no real significance. I was struck at that hearing, which Chairman Cruz called under the title "A War on Police," that that hearing actually produced no evidence that there is any meaningful organized war on police. And as the Co-Chair of the Senate Law Enforcement Caucus, I know that law enforcement faces real chal-

allenges nationally every day, but I see little evidence to suggest that these issues stem from the calls of some in the civil rights community for greater accountability. In fact, my experience at the local level was that police officers are some of the greatest advocates for accountability because it makes them more effective police officers.

So, is it your view that the protection of American civil rights is actually inconsistent with good policing and officer safety? Or do you see them as being fundamentally in harmony?

Director COMEY. Oh, they are fundamentally in harmony. Scrutiny and oversight and accountability are good for everybody, law enforcement and non-law enforcement.

Senator COONS. Well, thank you, Director. It's my view that in a democracy the enormous power that we give to law enforcement and the very high expectations we have for them are only strengthened by accountability that then produces community engagement, community support. The agency I was fortunate enough to be closely associated with for a decade really was an early national leader in community policing and did, I think, an outstanding job at winning the trust of our community and, thus, being effective at policing. And, I think, there is a lot of work to go in terms of accountability and engagement and protecting civil rights, but I appreciate your response on all four of the questions I have asked today, and I am grateful for your service. Thank you, Director.

Director COMEY. Thank you, Senator.

Chairman GRASSLEY. I have got three questions I would like to ask, and then I assume everybody has asked questions once and that nobody will come back.

I want to start by underlining what Senator Cornyn said about the Clinton email investigation. Almost 1,000 emails contained classified information were transmitted through and stored in the non-Government server system. A former IT specialist at the State Department who also managed the private server has avoided this Committee's questions by relying on the Fifth Amendment right of self-incrimination. And in the course of the FBI's investigation, there might come a time when it refers the matter to the Department of Justice for prosecution of some of the individuals involved.

But as you know, no matter what the FBI finds, a political appointee at the Justice Department will ultimately make the decision of whether or not to prosecute. That's why some have called for a special counsel to be appointed for an independent decision.

So, my question is, if the FBI refers the matter to the Justice Department but the Justice Department refuses to prosecute, the public will not learn the facts that the FBI independently inquiry established. So, would there be a process by which you would inform the public of what the FBI learned and what you will do if the decision not to prosecute appears to be improperly influenced by political considerations?

Director COMEY. Mr. Chairman, I am not comfortable answering a question about what might happen in that particular matter. I think it's important that I am—I'm making sure it has the right resources, the right people, and it's done in an expeditious, fair, and competent way. I don't want to speculate and go down that road, if I could.

Chairman GRASSLEY. Could I remind you that in the anthrax case, after the person that was suspected committed suicide, the FBI did make that investigation public? So, wouldn't there be a precedent for you making your investigation public?

Director COMEY. There is a variety of precedents for investigations, describing some or all of it to the public. I just don't want to start to speculate on this particular investigation.

Chairman GRASSLEY. Okay. State Department officials—along the same lines, State Department officials have informed my staff that the FBI has seized or taken possession of the State Department computer used by the witness who is asserting the Fifth Amendment to this Committee. There has also been a public report that the FBI has taken possession of State Department email servers. Is that correct? Has the FBI seized or taken possession of these State Department computers?

Director COMEY. I can't comment on that given that it is an ongoing matter.

Chairman GRASSLEY. I'm not really asking you what it serves. I am just asking you, do you have these tools available?

Director COMEY. Well, if I were to answer, I would be answering about what evidence we have gathered in an investigation. I can assure you—

Chairman GRASSLEY. You don't need to go any further.

Director COMEY. Okay.

Chairman GRASSLEY. I trust you. The American people rely upon you to investigate potential criminal conduct, and in the course of that conduct, politics cannot interfere with your responsibilities. In a "60 Minutes" interview, President Obama declared in response to a question about Secretary Clinton's use of a private server, quote, "I can tell you that this is not a situation in which America's national security was endangered," end of quote. How can you assure the American people that you will not let the White House influence the FBI's inquiry?

Director COMEY. I hope that the American people know the FBI well enough and the nature and character of this organization to know, as I have said many times, we don't give a rip about politics. Anybody's view of that investigation they are not involved in is irrelevant. We care about finding out what is true and doing that in a competent, honest, and independent way. I promise you that is the way we conduct ourselves.

Chairman GRASSLEY. Okay. Now, I would like to discuss whistleblowers, and the second of at least three questions I would like to ask you.

In your confirmation hearing, you expressed strong support for whistleblowers and the need for them to feel free to raise their concerns up their chain of command. FBI policy encourages employees to report wrongdoing to their supervisors. First question, do you support legal protections for FBI employees who follow FBI's own policies and report wrongdoing to their supervisors? If not, why not?

Director COMEY. I do, very much.

Chairman GRASSLEY. Okay. Under current law, FBI agents have no legal protection for reporting wrongdoing to their supervisors. Do you see any justification for not fixing that problem?

Director COMEY. I think it is very, very important that we create the safe zones that all of our people need to raise concerns that they might have. And so, that is the way I not only talk; that is the way I walk at the FBI. And I know that we are having conversations about are there additional protections we can offer. I think there might be sensible ways to do that. I have some small concerns. I want to make sure that we don't create a system where, to get too deep into the weeds here, an FBI agent or FBI employee can report not just fraud, waste, and abuse, but can get whistleblower protection for reporting bad management. That is potentially a huge range of things, so I want to be thoughtful about what we're considering whistleblowing as we do this. But I am open to try and improve the way we approach it.

As I said, I have tried to really walk this talk by the way I have acted, the people I have met with, the way I have given out awards in the FBI. And so, I will continue to work with you to try and improve that.

Chairman GRASSLEY. You've spoken repeatedly about ISIS' sophisticated and successful use of the internet to lure Americans to Syria and to inspire tacts—tactics in the United States. This is very concerning, and I know you speak from your heart on that.

Other than addressing the problem by encryption, are there any other tools that would help the FBI identify and monitor terrorists online? More specifically, can you explain what electronic communications and transactional records, or ECTR, I think that is referred to as an acronym, are and how Congress accidentally limited the FBI's ability to obtain them—obtain them or drafting them? Would fixing this problem be helpful for your counterterrorism investigations?

Director COMEY. It would be enormously helpful. There is essentially a typo in the law that was passed a number of years ago that requires us to get records, ordinary transaction records that we can get in most contexts with a non-court order because it doesn't involve content of any kind, to go to the FISA Court to get a court order to get these records. Nobody intended that. Nobody I've heard thinks that is necessary. It would save us a tremendous amount of work hours if we could fix that, without any compromise to anyone's civil liberties or civil rights. Everybody who has stared at this has said that is actually a mistake, we should fix that.

Chairman GRASSLEY. Yes. This will be my last question. I've—you heard my concerns about noncitizens who are not legal permanent residents buying and possessing guns in this country—if you want me to ask this, then I am not going to ask this other question. Let me go to this question.

In regard to your last response, you said you try to walk the talk on this. So, why hasn't the FBI imposed discipline in any of some cases that I have been investigating? What message does it send to FBI employees when the FBI fails to hold retaliators accountable for their actions? That will be my last question.

Director COMEY. That's a good question and a hard question. I believe we do work very hard to try and hold retaliators accountable. Each case—the challenge of answering it in the abstract level is each case has to be looked at individually. So, I do think that we work very hard to try and hold people accountable.

Now, often when people know we are coming for them, they will retire on us and leave Government service, which is a challenge. But it is not just that enforcement that matters. It's how do we act, how do we conduct ourselves. And I don't want to brag on myself, but I will for a second. We have Annual Directors Awards, and at the end of the Directors Awards this year, I gave an award to recognize somebody for blowing the whistle on misconduct. And I went back to the podium, and I said, "This matters. The reason I am saving this one for last is this matters. We are an organization dedicated to finding the truth in American life. We have to make sure we are open to seeing the truth about ourselves."

So, look, we're not perfect, and I think we can benefit from working with you to get better. But I believe we have sent the message this matters.

Chairman GRASSLEY. Listen, you have been here a long time. I thank you for the time you have given us. Maybe some Members will submit questions for answer in writing. I may even do that myself. I hope you will respond appropriately and as quickly as you can. Thank you very much for your service.

Director COMEY. Thank you, Senator.

[Whereupon, at 12:50 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#####



Department of Justice

**STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE**

**FOR A HEARING REGARDING
OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION**

**PRESENTED
DECEMBER 9, 2015**

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

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

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

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

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

National Security

Counterterrorism

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

The terrorist threat has changed in two significant ways. First, the core al Qaeda tumor has been reduced, but the cancer has metastasized. The progeny of al Qaeda—including AQAP, al Qaeda in the Islamic Maghreb, and the Islamic State of Iraq and the Levant (ISIL)—have become our focus. Second, we are confronting the explosion of terrorist propaganda and training on the Internet. It is no longer necessary to get a terrorist operative into the United States to recruit. Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change from a decade ago.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI and the Intelligence Community as a whole.

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

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

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life—from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is also seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging.

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

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

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

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

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

The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence about the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing; in partnership with our many federal, state, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue technological and other methods to help stay ahead of threats to the homeland.

Going Dark

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

The United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. Though the Administration has decided not to seek a legislative remedy at this time, we will continue the productive conversations we are having with private industry, State, local, and tribal law

enforcement, our foreign partners, and the American people. The FBI thanks the committee members for their engagement on this crucial issue.

Intelligence

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken steps to improve this integration. First, we have established an Intelligence Branch within the FBI headed by an executive assistant director (EAD). The EAD looks across the entire enterprise and drives integration. Second, we now have special agents and intelligence analysts at the FBI Academy engaged in practical training exercises and taking core exercises together. As a result, they are better prepared to work well together in the field. Third, we've made it a priority to focus on intelligence integration training for all levels of the workforce to ensure they have the tools needed to implement, manage, and maintain successful integration of intelligence and operations. Our goal every day is to get better at using, collecting, and sharing intelligence to better understand and defeat our adversaries.

The FBI cannot be content to just work the matters directly in front of us. We must also look beyond the horizon to understand the threats we face at home and abroad and how those threats may be connected. Toward that end, we gather intelligence, consistent with our authorities, to help us understand and prioritize identified threats, and to reveal the gaps in what we know about these threats. We then seek to fill those gaps and learn as much as we can about the threats we are addressing and others on the threat landscape. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to organize threats into priorities for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

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

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

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

Counterintelligence

We still confront traditional espionage—spies posing as diplomats or ordinary citizens. But espionage also has evolved. Spies today are often students, researchers, or businesspeople operating front companies. And they seek not only state secrets, but trade secrets, intellectual property, and insider information from the federal government, U.S. corporations, and American universities. Foreign intelligence entities continue to grow more creative and more sophisticated in their methods to steal innovative technology, critical research and development data, and intellectual property. Their efforts seek to erode America's leading edge in business, and pose a significant threat to our national security.

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

To combat this threat, the FBI's Counterintelligence Division has undertaken several initiatives. We directed the development, deployment, and operation of the Hybrid Threat Center (HTC) to support Department of Commerce Entity List investigations. The HTC is the first of its kind in the FBI; it has been well-received in the U.S. Intelligence Community, multiple FBI divisions, and the private sector.

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

Finally, the Counterintelligence Division and the Office of Public Affairs collaborated to conduct a joint media campaign regarding the threat of economic espionage. As a result of this collaboration, the FBI publicly released a threat awareness video called *The Company Man: Protecting America's Secrets*. This video is available on the FBI's public website and was shown more than 1,300 times across the United States by the

Counterintelligence Division's Strategic Partnership Coordinators to raise awareness and generate referrals from the private sector.

Cyber

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

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

We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. For example, as the committee is aware, the Office of Personnel Management (OPM) discovered earlier this year that a number of its systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective federal government employees, as well as other individuals for whom a federal background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

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

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

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

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

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

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

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

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

Through CyWatch, our 24-hour cyber command center, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion. We also work with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance. And we are training our state and local counterparts to triage local cyber matters, so that we can focus on national security issues.

Weapons of Mass Destruction

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

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

Criminal

We face many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent crime and public corruption. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to our security and safety in communities across the nation.

Public Corruption

Public corruption is the FBI's top criminal priority. The threat—which involves the corruption of local, state, and federally elected, appointed, or contracted officials—strikes at the heart of government, eroding public confidence and undermining the strength of our democracy. It impacts how well U.S. borders are secured and neighborhoods are protected, how verdicts are handed down in court, and how well public infrastructure such as schools and roads are built. The FBI is uniquely situated to address this threat, with our ability to conduct undercover operations, perform electronic surveillance, and run complex cases. However, partnerships are critical and we work closely with federal, state, local, and tribal authorities in pursuing these cases.

One key focus is border corruption. The federal government protects 7,000 miles of U.S. land border and 95,000 miles of shoreline. Every day, more than a million visitors enter the country through one of the 327 official Ports of Entry along the Mexican and Canadian borders, as well as through seaports and international airports. Any corruption at the border enables a wide range of illegal activities along these borders, potentially placing the entire nation at risk by letting drugs, guns, money, and weapons of mass destruction slip into the country, along with criminals, terrorists, and spies. Another focus concerns election crime. Although individual states have primary responsibility for conducting fair and impartial elections, the FBI becomes involved when paramount federal interests are affected or electoral abuse occurs.

Civil Rights

The FBI remains dedicated to protecting the cherished freedoms of all Americans. This includes aggressively investigating and working to prevent hate crime, “color of law” abuses by public officials, human trafficking and involuntary servitude, and freedom of access to clinic entrances violations—the four top priorities of our civil rights program. We also support the work and cases of our local and state partners as needed.

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

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

Health Care Fraud

We have witnessed an increase in health care fraud in recent years, including Medicare/Medicaid fraud, pharmaceutical fraud, and illegal medical billing practices. Health care spending currently makes up about 18 percent of our nation's total economy. These large sums present an attractive target for criminals. Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, and every taxpayer who funds Medicare is a victim. Schemes can also cause actual patient harm, including subjecting patients to unnecessary treatment or providing substandard services and supplies. As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used appropriately and not to line the pockets of criminals.

The FBI currently has over 2,700 pending health care fraud investigations. Over 70 percent of these investigations involve all government funded programs to include Medicare, Medicaid, CHIP, VA, DoD, and other U.S. government funded programs. As part of our collaboration efforts, the FBI maintains investigative and intelligence sharing partnerships with government agencies such as other Department of Justice components, Department of Health and Human Services, the Food and Drug Administration, the Drug Enforcement Administration, State Medicaid Fraud Control Units, and other state, local, and tribal agencies. On the private side, the FBI conducts significant information sharing and coordination efforts with private insurance partners, such as the National Health Care Anti-Fraud Association, the National Insurance Crime Bureau, and private insurance investigative units. The FBI is also actively involved in the Health Care Fraud Prevention Partnership, an effort to exchange facts and information between the public and private sectors in order to reduce the prevalence of health care fraud.

Violent Crime

Violent crimes and gang activities exact a high toll on individuals and communities. Today's gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit their illegal activities to single jurisdictions or communities. The FBI is able to work across such lines, which is vital to the fight against violent crime in big cities and small towns across the nation. Every day, FBI special agents work in partnership with state, local, and tribal officers and deputies on joint task forces and individual investigations.

FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces—focus on identifying and targeting major groups operating as criminal enterprises. Much of the Bureau's criminal intelligence is derived from our state, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and our sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups

engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

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

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

Despite these efforts, there is something deeply disturbing happening all across America. The latest Uniform Crime Reporting statistics, *Crime in the United States, 2014*, show that the number of violent crimes in the nation decreased, but this year we are seeing an uptick of homicides in some cities. The police chiefs in these cities report that the increase is almost entirely among young men of color, at crime scenes in neighborhoods where multiple guns are recovered. There are a number of theories about what could be causing this disturbing increase in murders in our nation's cities. We simply do not know for sure.

Need for Incident-Based Crime Data

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

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

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

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

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

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

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

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

Transnational Organized Crime

More than a decade ago, the image of organized crime was of hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or states, but organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion dollar schemes from start to finish. These criminal enterprises are flat, fluid networks with global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identity theft, trafficking of women and children, and other illegal activities. Preventing and combating transnational organized

crime demands a concentrated effort by the FBI and federal, state, local, tribal, and international partners. The Bureau continues to share intelligence about criminal groups with our partners and to combine resources and expertise to gain a full understanding of each group.

Crimes Against Children

The FBI remains vigilant in its efforts to eradicate predators from our communities and to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA, trace evidence, impression evidence, and digital forensics. Through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world, and these outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate both parents and children about the dangers posed by predators and to recover missing and endangered children should they be taken. Through our Child Abduction Rapid Deployment Teams, Innocence Lost National Initiative, Innocent Images National Initiative, annual Operation Cross Country, Office for Victim Assistance, 71 Child Exploitation Task Forces, and numerous community outreach programs, the FBI and its partners are working to keep our children safe from harm.

Operation Cross Country, a nationwide law enforcement action focusing on underage victims of prostitution, completed its ninth iteration during the first full week of October. Over 300 operational teams from over 500 agencies across 135 cities and 53 FBI Field Offices were instrumental in recovering child victims of all races and arresting pimps and customers. Ninety victim specialists, in coordination with local law enforcement victim advocates and non-governmental organizations, provided services to child and adult victims. .

The FBI established the Child Sex Tourism Initiative to employ proactive strategies to identify U.S. citizens who travel overseas to engage in illicit sexual conduct with children. One such undercover investigation led to the conviction earlier this year of an Alaskan man who produced child pornography in Cambodia and brought it to the United States, and who helped others plan to abuse children abroad.

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

Indian Country

There are 566 federally recognized Indian tribes in the United States, with the FBI and the Bureau of Indian Affairs having concurrent jurisdiction for felony-level crimes on over 200 reservations. According to the 2010 Census, there are nearly five million people living on over 56 million acres of Indian reservations and other tribal lands. Criminal jurisdiction in these areas of our country is a complex maze of tribal, state, federal, or concurrent jurisdiction.

The FBI's Indian Country program currently has 124 special agents in 34 FBI field offices primarily working Indian Country crime matters. The number of agents, the vast territory, the egregious nature of crime being investigated, and the high frequency of the violent crime handled by these agents makes their responsibility exceedingly arduous. The FBI has 14 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country, and we continue to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska Natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations concern homicide, crimes against children, or felony assaults.

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

Active Shooter Training

In response to the Sandy Hook school shooting, the president took steps to protect children and communities by reducing gun violence. He assigned the vice president to lead the effort with a focus on schools, institutions of higher education, and houses of worship. The FBI was assigned to lead law enforcement training to ensure coordination among agencies. To that end, we have trained more than 11,000 senior state, local, tribal, and campus law enforcement executives at conferences hosted by FBI field offices, and we have trained more than 7,000 first responders through tabletop exercises designed around facts similar to recent school shootings. To date, the FBI has provided our Advanced Law Enforcement Rapid Response Training course, an active shooter training program, to more than 31,500 officers from 5,600 agencies.

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

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

Five Eyes Law Enforcement Group

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

FBI Laboratory

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

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

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

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

Additionally, the Laboratory Division maintains a capability to provide forensic support for significant shooting investigations. The Laboratory Shooting Reconstruction Team provides support to FBI field offices by bringing together expertise from various Laboratory components to provide enhanced technical support to document complex shooting crime scenes. Services are scene and situation dependent and may include mapping of the shooting scene in two or three dimensions, scene documentation through photography, including aerial and oblique imagery, 360 degree photography and videography, trajectory reconstruction, and the analysis of gunshot residue and shot patterns. Significant investigations supported by this team include the shootings in Chattanooga, the Charleston church shooting, the shootings at the Census Bureau and NSA, the shooting death of a Pennsylvania State Trooper, the Metcalf Power Plant shooting in San Francisco, and the Boston Bombing/Watertown Boat scene.

Information Technology

The Information and Technology Branch provides information technology to the FBI enterprise in an environment that is consistent with intelligence and law enforcement capabilities, and ensures reliability and accessibility by members at every location at any moment in time. Through its many projects and initiatives, it is expanding its information technology (IT) product offerings to better serve the operational needs of the agents and analysts and raising the level of services provided throughout the enterprise and with its counterparts in the law enforcement arena and Intelligence Community.

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

FBI special agents and analysts need the best technological tools available to be responsive to the advanced and evolving threats that face our nation. Enterprise information technology must be designed so that it provides information to operational employees rather than forcing employees to conform to the tools available. IT equipment must be reliable and accessible, as close to where the work is performed as possible. By doing so, the FBI will decrease the time between information collection and dissemination.

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

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

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

Conclusion

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

I look forward to answering any questions you may have.

Senator Cruz Questions for the Record for
James B. Comey, Jr., Director, Federal Bureau of Investigation
U.S. Department of Justice
Full Committee
“Oversight of the Federal Bureau of Investigation”
Wednesday, December 9, 2015, 10:00 a.m.

I. The National Security Threat of the Islamic State of Iraq and Syria¹

- During your testimony, you echoed concerns, expressed by Chairman Grassley, that members of the Islamic State of Iraq and Syria (ISIS) have the capacity to possibly forge U.S. passports, which obviously would pose additional challenges in our efforts to halt ISIS operatives from entering the United States and launching terrorist attacks.
- 1. **Have federal, state, or local law enforcement officials made any recent arrests of individuals who were attempting to enter the United States with forged U.S. passports in the last three years?**
- 2. **Does the FBI believe the Department of State’s recent decision to discontinue the issuance of visa page inserts for valid U.S. passports will be helpful?**
- There has been a substantial amount of discussion recently about the nature of the threat posed by ISIS.
- 3. **Does the FBI consider ISIS to be a radical Islamist threat?**
- 4. **If the FBI suspects that an individual within the United States is engaging in terrorism or otherwise supporting terrorist activity, does the FBI have the authority to view individuals’ publicly accessible social media accounts in the absence of a search warrant? Whether your answer is yes or no, please provide a detailed explanation.**

II. Federal Government Capacity to Vet Syrian² Refugees

- Significant concerns remain about the inability of the United States government to properly vet Syrian refugees – and such concerns are only heightened in the wake of the December 2 terrorist attack in San Bernardino, California, where an individual who was vetted far more thoroughly than Syrian refugees was able to be approved for entry despite her radicalized background and other questions. You yourself previously expressed explicit concern about how little information we are likely to obtain about some of the individuals from (or traveling through) Syria.³

¹ If answers to any of these questions can only be answered in a classified setting, please contact the Committee to make arrangements for a classified briefing.

² The Committee is aware that some or many of the refugee population emerging from Syria are not Syrian nationals. For the sake of brevity and convenience, the entire refugee population will be referred to as Syrian refugees.

³ See Chuck Ross, *FBI Director Admits US Can’t Vet All Syrian Refugees for Terror Ties*, DAILY CALLER (Oct. 21, 2015) (quoting you as saying that, “if someone has never made a ripple in the pond in Syria in a way that would get

Senator Cruz Questions for the Record for
James B. Comey, Jr., Director, Federal Bureau of Investigation
U.S. Department of Justice
Full Committee
“Oversight of the Federal Bureau of Investigation”
Wednesday, December 9, 2015, 10:00 a.m.

1. Does the FBI have any access to local, municipal, or provincial records in Syria?
2. Does the FBI receive any records or information collection assistance from Syria’s national government?
3. Does the FBI have any shareable information about whether ISIS and/or other international terrorist organizations are specifically recruiting individuals who would not register on domestic or international crime or terrorism databases (so as to avoid detection)?

III. Private-Sector Encryption and Its Role in Preventing Anti-Terrorism Efforts

- During your testimony, you spoke of the law enforcement challenges created by some mobile technology companies that have refused to facilitate lawful access to encrypted data. While you were generally positive about the cooperation of some of these companies, members of the Committee are fully aware that other companies have been hostile to law enforcement efforts and been entirely uncooperative. Inexplicably, some of these companies have even refused to cooperate with the Department of Justice and the FBI when presented with a federal search warrant.
1. It is my understanding that Syed Rizwan Farook, who was one of the two radical Islamists who massacred 14 Americans in San Bernardino, California, on December 2, 2015, is known to have communicated with an unidentified international terror suspect. You specifically noted in your testimony that Farook had exchanged more than 100 messages with this unidentified individual, but that, because of the encryption challenges presented by Farook’s data provider, you are unable to obtain additional data that could save lives.
 - a. Please name the private-sector company or companies that are preventing you from obtaining the encrypted information on Farook’s mobile device.
 - b. Can any of the companies or individual leaders of these companies be criminally prosecuted by the Department of Justice for obstruction of justice? **If possible, please identify current provisions of Title 8 that could be applied to these situations.**

their identity or their interest reflected in our database, we can query our database until the cows come home, but there will be nothing show up [sic] because we have no record of them”).

NOTE: The Honorable James B. Comey Jr.’s responses to questions for the record are classified and are, therefore, provided separately.

Senator Cruz Questions for the Record for
James B. Comey, Jr., Director, Federal Bureau of Investigation
U.S. Department of Justice
Full Committee
“Oversight of the Federal Bureau of Investigation”
Wednesday, December 9, 2015, 10:00 a.m.

- c. Please inform the Committee if there is anything we can do to assist the FBI in terms of facilitating cooperation from the company or companies that are not cooperating with the FBI (in this case and other cases). **If possible, please recommend specific statutory changes that Congress can implement via legislation.**
2. It is my understanding that, particularly in abduction and missing persons situations, the inability to quickly get to data stored on mobile devices can literally mean the difference between life and death in some cases. Please elaborate on the subject of how important quick, legal access to data on mobile devices can be in the successful resolution of abduction and missing person cases.

IV. FBI Crime Scene and Evidence Collection Procedures

- On December 4, 2015, several news outlets provided live television coverage of reporters, camera crews, and other unidentified individuals digging through the belongings of the deceased San Bernardino terrorists, Syed Rizwan Farook and Tashfeen Malik. The coverage was somewhat startling in that it showed non-law enforcement digging through materials (which included credit cards, driver’s licenses, and books) that arguably still had investigative or informational value.
 - Later that day, FBI representatives responded to questions about the terrorists’ residence by stating, in substance, that the FBI had retrieved everything from the residence that it believed had evidentiary value, took a full inventory of the removed items, and turned the premises back over to the landlord.
1. **Is it standard operating procedure for the FBI to leave behind materials that might not be of obvious evidentiary value, but could at some point have evidentiary value?**
 2. **Please provide any additional, relevant information about the FBI’s crime scene and evidence collection procedures that may shed light on the events of December 4.**

**Senate Judiciary Committee
Hearing on Oversight of the Federal Bureau of Investigation
Questions from Senator Dick Durbin for Director James B. Comey, Jr.**

1. Attorney General Loretta Lynch recently denounced the “disturbing rise in anti-Muslim rhetoric” and stated that her “greatest fear as a prosecutor... is that the rhetoric will be accompanied by acts of violence.”

In recent weeks a Muslim member of Congress reportedly received a death threat; vandals allegedly defaced a mosque near Austin, Texas; and a man was arrested for breaking into a Florida mosque and damaging property. A sixth-grade girl in New York City was allegedly called “ISIS” as a group of boys punched her and tried to remove her hijab. And on Thanksgiving Day, a Muslim cab driver in Pittsburgh was shot in the back by a passenger who reportedly asked the driver about ISIS and whether he was a “Pakistani guy.”

Do you share the Attorney General’s concern that anti-Muslim rhetoric can lead to violence against the Muslim-American community? What steps is the FBI taking to protect the Muslim-American community and investigate alleged anti-Muslim hate crimes?

2. On October 15, 2015, I sent you a letter regarding a public service announcement that the FBI posted on October 8 entitled “New Microchip-Enabled Credit Cards May Still Be Vulnerable To Exploitation By Fraudsters.” The FBI withdrew this advisory on October 9 and issued a revised version of the advisory on October 13. In my letter I asked you to provide important information to help consumers and the general public understand and avoid payment card fraud. I received a response from the FBI dated December 3, but the response failed to answer the questions I asked. Please answer the following questions.
 - a. What is the annual dollar amount of payment card fraud associated with lost and stolen cards in the United States?
 - b. What is the annual dollar amount of lost-and-stolen payment card fraud that could be averted if all U.S. payment card transactions were capable of being authenticated with a Personal Identification Number (PIN), as is currently the case with ATM withdrawals?
 - c. In your view, is enabling a payment card with the option of PIN authentication an effective step to help reduce the occurrence of, and costs from, fraud in relation to payment card transactions?
 - d. Payment cards are now being issued in the United States with microchips pursuant to the Europay MasterCard Visa (EMV) security standard. EMV is a set of security specifications established by EMVCo, an organization owned and run by six giant payment card networks: American Express, Discover, MasterCard, Visa, JCB (a Japanese-based payments company) and UnionPay (a Chinese bankcard association). EMVCo is essentially the payment card industry’s effort to establish its own standard for card security technology. Is the FBI evaluating the security specifications established by EMVCo to ensure that these specifications are adequately protecting U.S. consumers against fraud?

NOTE: The Honorable James B. Comey Jr.’s responses to questions for the record are classified and are, therefore, provided separately.

- e. Is the FBI aware that payment card networks and banks in the United States may have an incentive to dissuade consumers and merchants from using PINs because the fees that networks and banks receive on non-PIN transactions are higher than on PIN transactions?
- f. The FBI's revised October 13 advisory states that "currently, not all EMV cards are issued to consumers with the PIN capability and not all merchant PoS (Point of Sale) terminals can accept PIN entry." Do you believe that fraud involving lost and stolen cards would be reduced if EMV cards were issued to consumers with PIN capability and if merchant PoS terminals were able to accept PIN entry?

NOTE: The Honorable James B. Comey Jr.'s responses to questions for the record are classified and are, therefore, provided separately.

**Hearing before the Senate Committee on the Judiciary
“Oversight of the Federal Bureau of Investigation”
Questions for the Record Submitted by Senator Al Franken**

Questions for Director James Comey:

Question 1. Terrorist recruitment has been an issue in Minnesota for some time, starting before I came to office—first with al Shabaab and, more recently, with ISIL. This is an issue I have been focused on since I came into office, and we must do everything we can to prevent ISIL from recruiting young people here at home. This issue continues to pose challenges for our state—both for law enforcement, and for the Minnesota families devastated by the loss of young men who have disappeared, some of whom were later found to have traveled to Syria.

I have urged the Department of Justice to invest in projects designed to counter violent extremism in the United States, and to focus resources on the places where those efforts are needed most. At the same time, I have pressed the administration to ensure that their work to counter violent extremism proceed with the input and cooperation of the communities affected. The government’s efforts are much more likely to be successful if they meaningfully engage the local community. It is essential that the community feel confident that the government’s efforts do not involve racial or ethnic profiling, and are not mere pretexts for surveillance and monitoring. Minnesota is home to the nation’s largest Somali-American population—a vibrant community that I’m proud to represent in the Senate—and it is important that our efforts to combat recruitment and radicalization not have the effect of scapegoating an entire community based on the actions of a few individuals.

How would you characterize the local community’s involvement and participation in the Bureau’s efforts to counter violent extremism? Does the FBI solicit and receive feedback from the community, and if so, how does the Bureau incorporate that feedback into the program?

Question 2. I recently wrote to both you and Attorney General Lynch expressing concern about an alarming spike in violence against members of the transgender community. To date, 22 transgender or gender non-conforming people have been the victims of homicide in 2015, and advocates who monitor attacks on the lesbian, gay, bisexual, and transgender (LGBT) community have described the current environment as a state of emergency.

Can you tell me what the Bureau is doing to investigate violent crimes targeting the LGBT community? And in your view, what more can the federal government do to prevent bias-motivated crime?

In the past you have commented on the need to improve the tracking and reporting of bias-motivated crimes by state and local law enforcement, which is currently not required by law. In your view, what more can be done to ensure that we have a fuller picture of the threats that many of our citizens face every day? And what steps is the FBI already undertaking?

NOTE: The Honorable James B. Comey Jr.’s responses to questions for the record are classified and are, therefore, provided separately.

Question 3. There has been an alarming increase in threats and violence directed at abortion providers and women's health centers this year. Health centers in Illinois, Kentucky, New Hampshire, and Washington have endured vandalism, arson, and other threats. And on November 27, three people lost their lives and nine more were wounded in a shooting at Planned Parenthood's Colorado Springs health center.

I understand that the FBI participates in the Justice Department's National Task Force on Violence Against Health Care Providers, which coordinates the federal investigation and prosecution of threats and violence directed toward abortion providers. What can you tell us about the steps the Bureau is currently taking—independently or in coordination with that body—to ensure that threats and violence not serve as barriers to safe and legal health care?

Question 4. In Minnesota, tribes have been working for years to access state and federal background check systems. Earlier this year, the Minnesota Legislature unanimously passed a state law authorizing this information sharing. The FBI Office of the General Counsel then determined that the Minnesota statute was overbroad and has not yet allowed tribes access to federal databases.

Tribes in Minnesota want to see this issue resolved. What can the FBI do to help tribes get access to these databases as intended by Minnesota law?

Question 5. In your written testimony you mention the FBI's 14 Safe Trails Task Forces. As part of the Headwaters Safe Trails Task Force, the FBI has deputized state-licensed law enforcement officers to carry out FBI responsibilities on the Red Lake Reservation in northern Minnesota. Red Lake is exempt from Public Law 280 so state law enforcement usually wouldn't have jurisdiction there. Deputizing state-licensed officers has created concerns that the state is being given jurisdiction over tribal land. Consequently, Red Lake has not signed the task force agreement. At the same time, Red Lake has real public safety needs and limited resources to deal with them.

How do we address the public safety needs of tribes like Red Lake while ensuring their sovereignty is respected?

NOTE: The Honorable James B. Comey Jr.'s responses to questions for the record are classified and are, therefore, provided separately.

Senate Committee on the Judiciary
Questions for the Record from Chairman Grassley
To James B. Comey, Jr.
Director, Federal Bureau of Investigation

1. Non-Citizens Purchase or Possession of Firearms in the U.S.

During our colloquy regarding suspected terrorists and the purchase of firearms, we discussed the different tools that the FBI has to stop a suspected terrorist from purchasing a gun. One of the avenues that you mentioned was determining if the suspected terrorist was *otherwise prohibited* from purchasing a firearm. We are currently looking at the issue of certain classes of aliens and their ability to purchase firearms under existing law.

- a. Would it help you in your counter-terrorism mission to narrow the class of non-citizens and non-lawful permanent residents that are permitted to purchase firearms?

Further, you were also asked “whether terrorist organizations around the world are aware of American gun laws.” After answering the question in the affirmative, the questioning senator read a statement from an al Qaeda spokesman that discussed the ease with which firearms can be purchased in America.

- b. Given our founding documents, specifically, the Bill of Rights, won’t the United States always be a place where our freedoms, including those preserved by the First, Second, Fourth, and Fifth Amendments create some degree of vulnerabilities?
- c. Put differently, as a free society, we are going to be more vulnerable than a dictatorial regime, correct?
- d. Finally, based upon your distinguished career in federal law enforcement, is it not also the case that prohibited criminals circumvent legitimate firearms retailers and obtain illegal guns?

2. Purchasing of Firearms

During your testimony, you were asked about firearms purchases from the internet. At the time of your testimony, you were unsure whether firearms could be directly shipped to an internet purchaser. It is my understanding those who purchase firearms on the internet must go to a federal firearms licensee to pick up their firearm and that firearms cannot be lawfully shipped directly to an internet purchaser.

- a. Is that also your understanding?
- b. Further, if an individual purchases a firearm from a commercial retailer on the internet, they will also have to fill out an ATF Form 4473 when they go to pick up the firearm and this will initiate the NICS check, correct?

NOTE: The Honorable James B. Comey Jr.’s responses to questions for the record are classified and are, therefore, provided separately.

You were also asked about gun violence in general and the specific issue posed by interstate transportation of firearms.

- c. It is my understanding that federal law enforcement, including ATF, regularly surveils gun shows through both overt and covert means and have recently stepped up these efforts and has successfully prosecuted cases stemming from this surveillance and interdiction. Is that accurate?

3. Cruise Ship Crime

Congress passed the Cruise Vessel Security and Safety Act of 2010 to address serious crimes that are committed against passengers on cruise ships, sometimes by passengers and sometimes by crew members. Passengers in international waters and away from land-based law enforcement can be vulnerable to such crimes and in a difficult jurisdictional position to report them and to seek to have prosecutions brought against perpetrators.

Despite the passage of this law, it is my understanding that only four such prosecutions have been brought under the law.

- a. What steps will the FBI take to make sure that additional prosecutions are brought under the Act?
- b. Do you believe that actions need to be taken to ensure that passengers are more aware of their rights under the Act?
- c. Can the FBI facilitate the ability of passengers to report crimes that can be prosecuted under the Act despite the logistical impediments that passengers aboard a cruise ship might face from the cruise line?

4. Need for More Reliable Information About Law Enforcement's Use of Lethal Force

Over the last few years, there have been a number of high profile uses of lethal force by law enforcement which resulted in the death of unarmed civilians. However, despite the focus on these incidents, there remains a lack of reliable data about them, in large part to the voluntary nature of the Uniform Crime Report system. You have publicly decried this lack of data.

In September 2015, I co-sponsored legislation with Senator Tim Scott aimed at addressing the absence of reliable data, the Walter Scott Notification Act of 2015. The bill would increase the data points to be collected (including participant demographics) from such lethal force incidents and decrease Byrne-JAG and COPS funding for state and local departments who fail to comply in their reporting.

The *Washington Post* recently published an article, "FBI to Sharply Expand System for Tracking Fatal Police Shootings," revealing that the FBI system for tracking fatal police shootings will be replaced in 2017 and dramatically expanded to capture details of incidents. The article indicated that the FBI would begin to track details of any incident in which a law enforcement officer

causes serious injury or death to a civilian (including the use of stun guns, pepper spray, and physical force). However, the new database will continue to rely on voluntary reports of local police departments.

- a. Please provide further details on the FBI's migration to the new database and its capabilities referenced in the above article.
- b. The bill I worked on with Senator Scott aims to incentivize local police departments to provide data to the FBI on the aforementioned incidents. What other options are the FBI and Bureau of Justice Statistics considering to make it easier for local law enforcement to report information for inclusion in the FBI database?

5. FBI Facilitation of Ransom Payments to Terrorist Organizations

In late April 2015, the Wall Street Journal reported that in 2012 the FBI helped facilitate a \$250,000 ransom payment to al Qaeda from the family of kidnapped aid worker Warren Weinstein.¹ The article alleged that although the FBI claimed it did not directly approve or authorize a ransom payment, it nonetheless “vetted a Pakistani middleman used by the family to transport the money and provided other intelligence to enable the exchange.”² The alleged ransom payment did not result in Dr. Weinstein's recovery, and he was instead reportedly killed by accident in a U.S. strike in January 2015.³ On May 1, 2015, I wrote to Attorney General Lynch to ask about the FBI's policies and practices regarding ransom payments in hostage recovery efforts.

On June 24, 2015, the White House released a “Report on U.S. Hostage Policy,” the result of an interagency review of the government's hostage recovery policies and procedures.⁴ That same day, President Obama also issued Presidential Policy Directive 30, “U. S. Nationals Taken Hostage Abroad and Personnel Recovery Efforts” (PPD-30) and Executive Order 13698, “Hostage Recovery Activities.”⁵ PPD-30, and its classified annex, superseded and revoked NSPD-12, “United States Citizens Taken Hostage Abroad,” which was issued in 2002.

PPD-30 and Executive Order 13698 set out a new hostage recovery framework within the government, including establishing a Hostage Recovery Fusion Cell (HRFC) to serve as the operational focal point for coordinating the recovery of U.S. hostages abroad. Although it is an interagency effort, the HRFC is located at FBI headquarters and its director is a senior FBI official. PPD-30 includes general policy disclaimers that “the United States Government will make no concessions to individuals or groups holding U.S. nationals hostage” as well as “[i]t is

¹ Adam Entous and Devlin Barrett, FBI Helped Facilitate Ransom for U.S. Hostage Killed in Drone Strike, THE WALL STREET JOURNAL, April 29, 2015. Available at <http://www.wsj.com/articles/fbi-helped-facilitate-ransom-for-u-s-hostage-killed-in-drone-strike-1430328084>

² *Id.*

³ Adam Entous, Damian Paletta, and Felicia Schwartz, *American, Italian Hostages Killed in CIA Drone Strike In January*, THE WALL STREET JOURNAL, April 23, 2015. Available at: <http://www.wsj.com/articles/american-italian-hostages-killed-in-cia-drone-strike-in-january-1429795801>

⁴ Available at https://www.whitehouse.gov/sites/default/files/docs/report_on_us_hostage_policy_final.pdf

⁵ Available at <https://www.whitehouse.gov/the-press-office/2015/06/24/presidential-policy-directive-hostage-recovery-activities> and <http://www.gpo.gov/fdsys/pkg/FR-2015-06-29/pdf/2015-16122.pdf> respectively.

United States policy to deny hostage-takers the benefits of ransom, prisoner releases, policy changes, or other acts of concession.” It also directed the HRFC to “coordinate efforts by participating departments and agencies to provide appropriate support and assistance to hostages and their families.” The Report on U.S. Hostage Policy clarified this, stating:

[F]amilies must understand what support the Government is able to offer consistent with this policy. For instance, the directive makes clear that U.S. policy does not prohibit engaging in communications with hostage-takers; specifically, the Government may itself communicate with hostage-takers, their intermediaries, interested governments, and local communities to attempt to secure the safe recovery of the hostage. The Government may also assist private efforts to communicate with hostage-takers to secure the recovery of a loved one, whether directly or through an intermediary; these efforts will be focused on ensuring the safety and security of a family to prevent them from being defrauded or further victimized by a hostage-taker.

Immediately after this description, the document states that “families understandably want to explore every option to secure their loved ones’ safe recovery” and that the Justice Department “does not intend to add to families’ pain in such cases by suggesting that they could face criminal prosecution” for material support of terrorism. Taken together, this seems to imply that the families are free to pay ransoms and that the HRFC, led by the FBI, will assist and ensure the families are not defrauded. Accordingly, several media outlets reported that the new policy made it easier for families to make ransom payments to terrorists.⁶

On October 6, 2015, DOJ sent its response to my May 1 letter. The response generally cited the public portions of PPD-30, and did not substantively answer any of the questions in the May letter. On December 14, 2015, members of the HRFC provided a classified briefing to Congressional staff. However, that briefing also left many of the questions from the May letter unanswered.

- a. Was the FBI involved in a payment of a ransom in an attempt to recover Dr. Weinstein?
- b. Did the FBI vet a Pakistani middleman for the Weinstein family to use in making a ransom payment to al Qaeda in an attempt to recover Dr. Weinstein?
- c. Did the FBI provide other intelligence to enable the ransom payment? If so, what intelligence was provided? To whom was it provided?
- d. What other steps, if any, did the FBI take to facilitate the ransom payment?

⁶ Yochi Dreazen and Lara Jakes, *Hostage Review Will Make It Easier for Families to Pay Ransoms*, FOREIGN POLICY, June 22, 2015. Available at <http://foreignpolicy.com/2015/06/22/hostage-review-will-make-it-easier-for-families-to-pay-ransoms/>; *Obama Clears Way for Hostages’ Families to Pay Ransom*, AL JAZEERA, June 25, 2015. Available at: <http://www.aljazeera.com/news/2015/06/obama-hostages-families-pay-ransom-150624214719222.html>

- e. What steps, if any, did the FBI take in preparation for a potential release of Dr. Weinstein following the ransom payment to secure his safe return to the United States?
- f. What happened to the ransom money after Dr. Weinstein was not released?
- g. What steps, if any, did the FBI take to secure a return of funds to the Weinstein family?
- h. Has the FBI been involved in any transfer of money in connection with attempts to secure the release of hostages held by al Qaeda, the Taliban, the Haqqani network, ISIS, or associated forces?
- i. Has the FBI been involved in any transfer of money in connection with “proof of life” requests relating to hostages held by al Qaeda, the Taliban, the Haqqani network, ISIS, or associated forces?
- j. If the answer to either questions h or i is yes, since 2009, which groups or individuals received such payments, and how much money did each receive?
- k. If the answer to either questions h or i is yes, since 2009, what procedures were used to approve the FBI’s role in such transfers, and which government officials approved the actions involved?
- l. Prior to the issuance of PPD-30, what were the FBI’s policies and procedures relating to ransom payments, whether by the U.S. Government or third parties, in hostage recovery efforts?
- m. Prior to the issuance of PPD-30, what audit procedures, if any, were in place to ensure FBI compliance with these policies, procedures, and all applicable law?
- n. What are the FBI’s current policies and procedures relating to ransom payments, whether by the U.S. Government or third parties, in hostage recovery efforts?
- o. What audit procedures, if any, are currently in place to ensure FBI compliance with these policies, procedures, and all applicable law?
- p. Have either these past or present audit procedures, if they exist, revealed any violation of FBI policies, procedures, or applicable law?
- q. Has the FBI otherwise learned of such violations?
- r. If any violations were found, what remedial or punitive actions were taken?

6. FBI Implementation of Obama Administration Policy on Drones

The FBI has previously acknowledged that it has a fleet of approximately 17 unmanned aircraft systems (UAS or drones). In February 2015, the Obama Administration issued a Presidential Memorandum on the use of drones by Federal agencies. The Memorandum requires federal agencies to enact policies concerning: (1) data collection and retention (including PII); (2) oversight issues, including the deployment of drones by Federal agencies in support of State, local, and tribal governments; and (3) transparency, to include providing notice to the public of drone operation areas and an annual public summary by each agency detailing the types of missions flown. What has the FBI done to implement the Memorandum?

7. FBI Crime Lab Shortcomings and Inconsistencies

On September 14, 2015, the FBI sent Committee staff a letter concerning its review of microscopic hair comparison cases. In that letter, the FBI noted that it has closed the review of 689 of these cases because it could not obtain a copy of the trial transcript. In briefings, Committee staff has learned that the FBI typically closes such cases after one or two letters have been sent and/or one or two phone calls have been made asking for the transcript. A person who may have been wrongly convicted due to shoddy FBI lab work should not sit in jail because the FBI failed to obtain and review a trial transcript to identify its error.

The Innocence Project, which is partnering with the FBI on its review, has suggested the FBI should send agents to follow up in person with law enforcement agencies and prosecutors who have failed to respond to the FBI. For their part, FBI lab officials informed Committee staff that using “investigative resources” in this review would require your office’s approval.

- a. Have you authorized FBI field offices to send agents in person to those jurisdictions that failed to respond to the FBI’s phone call and letter requests for copies of these transcripts?
- b. If the answer to Question (a) is “yes,” how many in-person visits have been conducted? If the answer to Question (a) is “no,” please explain why not, and also whether you will consider providing such authorization by a date certain.
- c. Please provide the name of each jurisdiction that has failed to answer the FBI’s inquiries for transcripts.
- d. The FBI has identified 21,600 cases prior to 2000 which may have been affected by problematic crime lab work. Committee staff has learned through briefings that the FBI’s review only dates back to 1985 because the FBI did not have computer records before then. In an October 29, 2015 letter, the Committee asked you to consider a systematic review of cases prior to 1985, and requested updates on any such efforts. What steps has the FBI taken to obtain information that would allow it to examine hair analyses that were conducted in cases prior to 1985?

8. FBI Use of Spyware and Proposed Change to Rule 41 FRCP

On June 12, 2015, I wrote you to ask for details about the FBI's use of spyware, also known as "network investigative techniques." I have yet to receive a response. While the FBI's use of spyware in general has long been reported, the details of its capabilities, as well the policies and procedures surrounding its usage, are unclear. According to press reports, spyware programs can be remotely deployed to a targeted computer to surreptitiously activate the computer's camera and microphone; collect passwords; search the computer's hard drive, random-access memory, and other storage media; generate latitude and longitude coordinates for the computer's location; and intercept phone calls, texts, and social media messages. It is a powerful surveillance tool whose use should be subject to oversight, and its increased use has been proposed as one means of combatting the "going dark" problems posed by encryption.

As briefly discussed in the Committee's oversight hearing with you in May of 2014, the Department of Justice is currently seeking to amend Federal Rule of Criminal Procedure 41 ("Rule 41") to allow the Department to deploy spyware more easily. Rule 41 applies to search and seizure warrants, and under the current version of the rule, federal prosecutors generally must seek a warrant in the judicial district in which the target of the search is located.^[1] This can be a difficult task in the context of cybercrime. The Justice Department's proposed changes would, under certain circumstances, allow judges to grant warrants for remote searches of computers located outside their district or when the location is unknown -- changes that would allow the FBI to more easily obtain approval to infiltrate computer networks to covertly install spyware.^[2] The proposed changes would not affect the requirement that, in order for the FBI to obtain a warrant under the rule, it must demonstrate probable cause that the targeted device contains evidence of a crime.

A number of organizations have raised concerns about the scope of the proposed rule change, including constitutional concerns, risks of forum-shopping, and potential extraterritorial use.^[3] Despite these concerns, the U.S. Courts' Judicial Conference Advisory Committee on Criminal Rules voted in favor of the change in March of this year, as did the next group in the review process, the Courts' Standing Committee, on May 28,^[4] followed by approval from the Judicial Conference on October 9.^[5] In keeping with the process for modifying the rules, the proposed change will next be considered by the Supreme Court, with a Congressional review period to follow.

^[1] Fed. R. Crim. P. 41(b)(1), subject to exceptions in Fed. R. Crim. P. 41(b)(2)-(5).

^[2] Dustin Volz, *FBI's Plan to Expand Hacking Power Advances Despite Privacy Fears*, NATIONAL JOURNAL, Mar. 16, 2015, available at <http://www.nationaljournal.com/tech/fbi-s-plan-to-expand-hacking-power-advances-despite-privacy-fears-20150316>.

^[3] Dustin Volz, *Google Calls FBI's Plan to Expand Hacking Power a 'Monumental' Constitutional Threat*, NATIONAL JOURNAL, Feb. 18, 2015; Stan Schroeder, *Proposed Rule Would Give U.S. Power to Cybersnoop Worldwide, Google Warns*, MASHABLE, Feb. 19, 2015.

^[4] Cory Bennett, *FBI Request to Expand Hacking Power Advances*, THE HILL, Mar. 17, 2015; Cory Bennett, *FBI Inches Closer to Expanded Search Powers*, THE HILL, May 29, 2015; Tim Cushing, *Judicial Committee Gives FBI The First OK It Needs To Hack Any Computer, Anywhere On The Planet*, TECHDIRT, Mar. 17, 2015.

^[5] <http://www.uscourts.gov/rules-policies/pending-rules-amendments>

Although the uses of stealthy surveillance and deception to catch criminals are lawful and well-recognized investigative tactics under certain circumstances, and although the FBI's use of spyware in general has long been reported,^[6] the Committee lacks the specific information about the FBI's current use of spyware necessary to fulfill the Committee's oversight responsibilities, including: the types of spyware programs used; their capabilities; the FBI's internal policies and procedures for using spyware; the legal processes used; the methods of deploying spyware; and the audit procedures used to ensure the spyware is used in compliance with both FBI policies and the law.

Publicly available information on the FBI's use of spyware is often inconsistent. It is unclear from public reporting which spyware programs the FBI currently uses and what their capabilities are. While some press reports have stated that FBI spyware merely logs a target's "IP address, MAC address, computer programs running, operating system details, browser details, and other identifying computer information,"^[7] a 2013 court order denying an FBI warrant application stated that the "application request[ed] authorization to surreptitiously install data extraction software [that] has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents."^[8] A Washington Post article also reported that the FBI's spyware can "covertly download files, photographs[,] and stored e-mails, or even gather real-time images by activating cameras connected to computers[.]"^[9] Similarly, while some press reports have described a spyware program developed in-house by the FBI,^[10] others have noted that the U.S. government is now the largest purchaser of malware from the private sector,^[11] and another component of the Justice Department (DEA) has acknowledged to the Committee that it purchased private-sector spyware.^[12]

- a. Which spyware, related programs, and other network investigative techniques has the FBI used in the field since 2009? Please include both government-created programs and ones purchased externally, if any, from companies such as Hacking Team and Gamma Group International.
- i. What are each program's capabilities?

^[6] Craig Timberg and Ellen Nakashima, *FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, THE WASHINGTON POST, Dec. 6, 2013; see Kevin Poulsen, *Documents: FBI Spyware Has Been Sharing Extortionists, Hackers for Years*, WIRED, Apr. 16, 2009.

^[7] Kate Knibbs, *The FBI Has Its Own Secret Brand Of Malware*, GIZMODO, April 2, 2015; Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED, July 18, 2007.

^[8] *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 755 (S.D. Tex. 2013); see Jennifer Valentino-DeVries, *Judge Denies FBI Request to Hack Computer in Probe*, THE WALL STREET JOURNAL, Apr. 24, 2013.

^[9] Craig Timberg and Ellen Nakashima, *FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, THE WASHINGTON POST, Dec. 6, 2013.

^[10] *Supra* n. 7.

^[11] Zack Whittaker, *U.S. Government Becomes the 'Biggest Buyer' of Malware*, ZDNET, May 13, 2013; see Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, REUTERS, May 10, 2013.

^[12] <http://www.judiciary.senate.gov/imo/media/doc/2015-7-14%20DOJ%20to%20Grassley%20%28DEA%20Software%29.pdf>

- ii. How much has the FBI spent on each program?
- iii. How many times has the FBI used each of these programs in the field, and in what capacity? How many times has the FBI used the programs to remotely activate the subject device's camera or microphone?

The procedures used by the FBI to obtain approval to deploy spyware and the methods of such deployment also raise important issues. The Washington Post has reported that FBI agents “obtain warrants to search a suspect’s computer but generally do not inform the judge of an intent to hack the computer to install the malware.”^[13] The Washington Post also reported that the most common delivery method for installing the spyware is phishing attacks, in which the FBI masquerades as a trustworthy source in order to trick the target into clicking on a link infected with the spyware.^[14] In one publicly-reported case, FBI agents posed as the Associated Press and created a fake AP news article in a successful phishing effort to deploy spyware.^[15] However, in the relevant search warrant application, the agents “did not alert the judge of their plan to mimic the media.”^[16] After learning of the ruse, the AP stated “[w]e find it unacceptable that the FBI misappropriated the name of the Associated Press and published a false story attributed to the AP. This ploy violated AP’s name and undermined AP’s credibility.”^[17] It is also unclear from public reporting whether the FBI uses other methods of spyware deployment in addition to phishing, such as zero-day exploits, which exploit vulnerabilities in legitimate software applications. However, a recent Washington Post article, featuring an interview with FBI personnel, stated that the FBI uses zero-day exploits.^[19]

- b. What are the internal FBI policies and procedures related to requesting, approving, deploying, and terminating the use of spyware and related programs? Please provide copies of all guidance documents.
- c. Pursuant to what legal authorities does the FBI deploy spyware and related programs?
 - i. Does the FBI always obtain a search warrant or other judicial approval prior to using such programs? If not, why not?
 - ii. Does the FBI use different legal authorities or processes based on the jurisdiction in which it determines the target to be located?

^[13] Ellen Nakashima and Paul Farhi, *FBI Lured Suspect With Fake Web Page, But May Have Leveraged Media Credibility*, THE WASHINGTON POST, Oct. 28, 2014.

^[14] Craig Timberg and Ellen Nakashima, *FBI’s Search for “Mo,” Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, THE WASHINGTON POST, Dec. 6, 2013.

^[15] *Supra* n. 13; see James B. Comey, *To Catch a Crook: The FBI’s Use of Deception*, Letter to the Editor, THE NEW YORK TIMES, Nov. 6, 2014.

^[16] *Supra* n. 13.

^[17] *Id.*

^[19] ^[19] Ellen Nakashima, *Meet the Woman In Charge of The FBI’s Most Controversial High-Tech Tools*, THE WASHINGTON POST, Dec. 8, 2015. (“Privacy advocates also worry that to carry out its hacks, the FBI is using [‘]zero-day[‘] exploits that take advantage of software flaws that have not been disclosed to the software maker. That practice makes consumers who use the software vulnerable, they argue. Hess acknowledged that the bureau uses zero-days — the first time an official has done so.”)

- iii. Does the FBI use different legal authorities or processes if it cannot determine the jurisdiction in which the target is located?
- d. Has the FBI deployed spyware on behalf of state or local law enforcement? If so, what are the internal FBI policies and procedures related to doing so?
- e. When the FBI seeks a warrant to search a computer, does it always notify the judge when it intends to hack the targeted computer and surreptitiously install spyware? Does it specify in the warrant application the capabilities of the spyware it seeks to deploy? Does it specify the method of deployment to be used?
- f. What methods does the FBI use to deploy spyware? Please list each method of deployment used in the field since 2009 and the number of times it has been used.
- g. Does the FBI use zero-day exploits in conjunction with its use of spyware?
 - i. If so, are these zero-day exploits developed by the government or purchased externally from private companies, such as Vupen Security?
 - ii. If so, how much has the FBI spent on developing or purchasing zero-day exploits? Please list both the cost for in-house development and external purchases.
 - iii. If so, does the FBI ever notify the company that owns the exploited software of the security breach? If it does, what policies guide the timing and content of this disclosure? If it does not, why not?
- h. As noted above, the FBI has acknowledged using phishing to deploy spyware, and impersonating a real media outlet in doing so. Since 2009, how many times has the FBI impersonated personnel from legitimate companies, whether media or otherwise, in deploying spyware?
 - i. Which companies has it impersonated?
 - ii. Does the FBI notify the companies it impersonates that it has done so? If so, what policies guide the timing and content of this disclosure? If not, why not?
- i. For how long does the FBI retain any data obtained through spyware?
 - i. Who has access to the data while it is in the FBI's possession?
 - ii. How, if at all, is the data destroyed?
- j. What internal audit procedures does the FBI use to ensure that spyware and related programs are used in accordance with agency policies, procedures, and the law?

- i. If they exist, have such internal audit procedures discovered any violations of FBI policies, procedures, or applicable law relating to the use of spyware or related programs? Has the FBI discovered any such violations through other means?
- ii. If so, please provide the details of each violation, as well as any remedial or punitive measures taken in response.

On July 15, 2015, I wrote you regarding public reports about FBI purchasing spyware from an Italian spyware company, Hacking Team. I have yet to receive a response from FBI. Earlier in July, Hacking Team was itself hacked, and a number of the company's internal emails and documents were leaked to the public. Subsequent reporting on the documents detailed Hacking Team's business relationships with the DEA, the FBI, and the DoD.^[20] In addition to Hacking Team's relationships with legitimate law enforcement and military buyers, it is troubling that the leaked documents also revealed Hacking Team's business relationships with a number of repressive regimes around the world, including Sudan.^[21] While it is vital that U.S. law enforcement and our military have the technological tools needed to investigate terrorists and criminals in order to keep the public safe, it is also important that we acquire those tools from responsible, ethical sources who are acting in accordance with the law. As you know, the Sudan Accountability and Divestment Act of 2007 ("the Act"), PL 110-174, and its implementing regulation, 48 CFR 25.702, prohibit the United States Government from entering into contracts with any contractor conducting certain types of restricted business with Sudan, including the sale of "military equipment," which the Act defines as:

- (A) weapons, arms, military supplies, and equipment that readily may be used for military purposes, [. . .]; or
- (B) supplies or services sold or provided directly or indirectly to any force actively participating in armed conflict in Sudan. PL 110-174.^[22]

^[20] E.g., Lorenzo Franceschi-Bicchierai, *Spy Tech Company "Hacking Team" Gets Hacked*, MOTHERBOARD, July 5, 2015; Cory Bennett, *Hack at Surveillance Firm Exposes Ties to FBI, DEA*, THE HILL, July 6, 2015; Cora Currier and Morgan Marquis-Boire, *Leaked Documents Show FBI, DEA, and U.S. Army Buying Italian Spyware*, THE INTERCEPT, July 6, 2015; Joseph Cox, *The FBI Spent \$775k on Hacking Team's Spy Tools Since 2011*, WIRED, July 6, 2015; Jennifer Valentino-Devries and Danny Yadron, *Hacking Team, the Surveillance Tech Firm, Gets Hacked*, THE WALL STREET JOURNAL, July 6, 2015.

^[21] Dell Cameron, *Hacking Team Sold Spy Tools to Oppressive Sudanese Government*, THE DAILY DOT, July 6, 2015; Lauren Walker, *Cybersecurity Company Supplies Repressive Regimes with Spyware, Recent Hack Claims*, NEWSWEEK, July 6, 2015; Shane Harris, *U.S. Hired Dictators' Favorite Hackers*, THE DAILY BEAST, July 6, 2015; Tim Cushing, *Hacking Team Hacked: Documents Show Company Sold Exploits and Spyware to UN-Blacklisted Governments*, TECHDIRT, July 6, 2015; Cora Currier and Morgan Marquis-Boire, *A Detailed Look at Hacking Team's Emails About Its Repressive Clients*, THE INTERCEPT, July 7, 2015; Jose Pagliery, *This Company Sells Spy Tools to Evil Governments*, CNN MONEY, July 6, 2015; Samuel Gibbs, *Hacking Team Boss: We Sold to Ethiopia But 'We're the Good Guys'*, THE GUARDIAN, July 13, 2015 (in an interview, Hacking Team founder "admitted providing tools to [...] Sudan").

^[22] Some spyware and other types of malware readily may be used for military purposes. See Department of Defense, *LAW OF WAR MANUAL, Chapter XVI: Cyber Operations* 994-1008, June, 2015. As explained in the Senate Report on the Sudan Accountability and Divestment Act of 2007, the Act's definition of restricted "military equipment" is meant to include "dual use" items unless "it can be credibly proven that these items will not be used for any military purpose." S. Rep. 110-213. Moreover, Hacking Team reportedly sold its spyware to Sudan's

In order to prevent the government from entering into such prohibited contracts, the Act requires the head of each executive agency to ensure that each contract entered into by the agency for the procurement of goods or services includes a clause that requires the contractor to certify that it does not conduct restricted business operations in Sudan. The Act further provides that if the head of a government agency determines that the contractor has submitted a false certification, he or she may impose remedies, including terminating the contract and debaring or suspending the contractor from eligibility for Federal contracts. Under the Act, the General Services Administrator is to include on the GSA's List of Parties Excluded from Federal Procurement each contractor that is debarred, suspended, proposed for debarment or suspension, or declared ineligible by the head of an executive agency on the basis of a determination of a false certification.

According to press reports, Hacking Team's business relationships with FBI and the Army began in 2011.[23] Hacking Team's internal documents reveal that in 2012 the company sold its spyware to Sudan's National Intelligence and Security Service for 960,000 euros, and that this relationship continued until late 2014.[24] In June of 2014, the United Nations panel monitoring the implementation of sanctions against Sudan began investigating Hacking Team's alleged contract with Sudan, writing to the company to seek information.[25] Hacking Team did not immediately respond. Months later, in November of 2014, internal Hacking Team documents stated that its business with Sudan was "unofficially suspended, on-hold." [26] In January of 2015, Hacking Team finally responded to the U.N., claiming—in the present tense—that the company has no "current sales relationship" with Sudan.[27] In a subsequent letter, Hacking Team reportedly argued that its spyware does not qualify as weaponized software that would run afoul of U.N. sanctions against Sudan. The U.N. disagreed, writing:

The view of the panel is that as such software is ideally suited to support military electronic intelligence (ELINT) operations it may potentially fall under the category of 'military ... equipment' or 'assistance' related to prohibited items. Thus its potential use in targeting any of the belligerents in the Darfur conflict is of interest to the Panel. [28]

National Intelligence Security Service. *Infra* n. 5. "[T]he head of National Intelligence Security Services [. . .] was among the key figures ordering and coordinating the violence in Darfur." Emily Wax, *U.S. Report Finds Sudan Promoted Killings; Use of Term 'Genocide' Debated Ahead of Powell Testimony on Darfur Atrocities*, THE WASHINGTON POST, Sep. 8, 2004.

[23] *Supra* n. 26.

[24] Cora Currier and Morgan Marquis-Boire, *A Detailed Look at Hacking Team's Emails About Its Repressive Clients*, THE INTERCEPT, July 7, 2015.

[25] *Id.*; see Tim Cushing, *Hacking Team Hacked: Documents Show Company Sold Exploits and Spyware to UN-Blacklisted Governments*, TECHDIRT, July 6, 2015. Hacking Team's suspected business with Sudan was first publicly noted in a 2014 report by Citizen Lab, which is based at the University of Toronto and researches the intersection of information technology and human rights. See Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, *Mapping Hacking Team's "Untraceable" Spyware*, THE CITIZEN LAB, Feb. 17, 2014.

[26] *Supra* n. 30.

[27] *Id.*; Cushing *supra* n. 31.

[28] *Id.*

The July leak of Hacking Team's internal documents seems to vindicate the U.N.'s suspicions, and after the leak Hacking Team's founder reportedly admitted the company's business with Sudan.^[29] Since the leak, at least one European official has also asked Italy and the European Commission to investigate whether Hacking Team's sales to Sudan and Russia violated European sanctions against those countries.^[30]

In light the reports of Hacking Team's business with FBI and Hacking Team's concomitant business with Sudan, the question arises as to whether the contracts the company or its resellers had with U.S. agencies were in violation of the Sudan Accountability and Divestment Act of 2007.

- k. Please describe in detail any contract, agreement, training, or other business the FBI has ever had with Hacking Team, its resellers, or its affiliated companies.^[31] Does the FBI or DoD currently have a business relationship with Hacking Team, its resellers, or its affiliated companies?
- l. In keeping with the requirements of the Sudan Accountability and Divestment Act of 2007, did the FBI's contracts for procurement of goods or services from Hacking Team, its resellers, or its affiliated companies include a clause requiring the contractor to certify that it does not conduct restricted business operations in Sudan? If so, please provide copies of all such contracts, including any contracts for licenses, training, upgrades, technical support, and renewal of services. If not, why not?
- m. If such certifications were included in the contracts, in light of the reports of Hacking Team's business relationship with Sudan, has FBI evaluated whether Hacking Team, its resellers, or its affiliated companies submitted a false certification? If so, please provide copies of all documents relating to such evaluations. If not, why not?
- n. If FBI has determined that the contracts with Hacking Team, its resellers, or its affiliated companies contained false certifications, have you taken any of the remedial actions provided in the Act, including terminating the contract and debarring or suspending Hacking Team from eligibility for future Federal contracts? Have you reported such determination to the Administrator of General Services so she may include Hacking Team on the List of Parties Excluded from Federal Procurement? If so, please provide copies of all documents relating to such remedial actions. If not, why not?

^[29] Gibbs *supra* n. 27 (in an interview, Hacking Team founder "admitted providing tools to [...] Sudan").

^[30] Lorenzo Franceschi-Bicchierai, *Italy Should Investigate Hacking Team, European Parliament Member Says*, MOTHERBOARD, July 7, 2015.

^[31] According to press reports, Hacking Team has used a variety of partner companies in selling its spyware. See Joshua Kopstein, *Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments*, MOTHERBOARD, July 9, 2015; Lorenzo Franceschi-Bicchierai, *The DEA Has Been Secretly Buying Hacking Tools From an Italian Company*, MOTHERBOARD, April 15, 2015.

- o. If you have determined that the contracts with Hacking Team, its resellers, or its affiliated companies contained false certifications with regard to Sudan, have you referred the matter to the appropriate sections of the Department of Justice to investigate whether such false certifications or the underlying business with Sudan constituted a criminal matter? If so, please provide copies of such referrals. If not, why not?

9. FBI Investigations of Fetal Tissue Transfers

In July 2015, the Center for Medical Progress began releasing a series of undercover videos relating to transfers of fetal tissue by Planned Parenthood to intermediary companies, which then transfer the tissue to researchers. The videos raised substantial questions about whether Planned Parenthood and the middle-man companies violated federal laws relating to fetal tissue, and the Committee began a wide-ranging inquiry in response.

While the vast majority of that inquiry has focused on the activities of Planned Parenthood and the middle-man companies with which it works, on August 27, 2015, I wrote to you and Attorney General Lynch to inquire about the government's enforcement of two of the key fetal tissue laws, 42 U.S.C. § 289g-1 and g-2, which were enacted in 1993. Under 42 U.S.C. § 289g-2, it is illegal for any person to knowingly acquire, receive, or otherwise transfer any human fetal tissue for valuable consideration. Under 42 U.S.C. § 289g-1, which applies in the context of research conducted or supported by the Department of Health and Human Services that relates to the transplantation of human fetal tissue for therapeutic purposes, it is illegal to alter of the timing, method or procedures used to terminate a pregnancy if the alteration was made solely for the purpose of obtaining the fetal tissue.⁷

My August 27th letter asked: how many times the FBI has investigated possible violations of these laws since they were enacted in 1993; how many of these investigations lead to prosecutions; how many prosecutions resulted in convictions; how many times FBI had received referrals, complaints, or tips alleging violations of these laws; whether FBI has any internal guidance documents relating to investigations of violations of these laws; and whether FBI is currently engaged in any active investigations of alleged violations. Additionally, the letter requested investigation files and associated materials relating to a publicly announced investigation in 2000-01 of an alleged violation. That investigation did not result in a prosecution, and the subject of the investigation has since died.

On November 5, 2015, the Department of Justice ("DOJ") sent a letter in response. DOJ stated that it will not comment on whether there are or are not any active investigations relating to 42 U.S.C. § 289g-1 and g-2. The letter also stated that, as far as DOJ can tell, since the enactment of the laws in 1993, there has not been a single prosecution for alleged violations of them. DOJ did identify two investigations of alleged violations of § 289g-2 that were undertaken, neither of which resulted in a prosecution. One of those was the investigation referred to by me in my letter. DOJ stated that they are reviewing the records of these investigations and will supplement

⁷ After sending the letter, we were informed by the Department of Health and Human Services that it has neither conducted nor supported any such research, which would trigger the law's requirements, since 2007.

their response once the review is complete. DOJ also stated that they do not keep records of how many referrals, complaints, or tips they received alleging violations of § 289g-2, nor do they have any internal guidance documents relating to investigations of violations of these laws.

- a. Will the FBI commit to actively investigating all credible referrals, complaints, or tips alleging violations of these federal fetal tissue laws?
- b. The Committee needs to evaluate whether these fetal tissue laws are being enforced as intended, and if they are not, to determine why not and what corrective action is necessary. Will the FBI provide the Committee with its investigative files, if any, relating to the two fetal tissue investigations referenced above? If not, why not?

10. FBI Whistleblowers and Protecting Disclosures to Supervisors

During the hearing on December 9, 2015, I asked you whether “you support legal protections for FBI employees who follow FBI’s own policies and report wrongdoing to their supervisors?” You responded, “I do, very much.”⁸ You also said that you are “open to try and improve the way we approach” FBI whistleblower protection.⁹

Senator Leahy and I introduced bipartisan legislation this month to fill in the gaps in protections for FBI whistleblowers. Among many other improvements, the bill offers protection for the first time to FBI whistleblowers who report wrongdoing to their supervisors and other management within their chain of command.

Will you commit to working with this Committee to make these important changes?

11. Accountability for Reprisal Against FBI Whistleblowers

In the hearing on December 9, 2015, I asked you about accountability for individuals who retaliated against FBI whistleblowers. According to a letter received from your office on December 1, 2015, during your tenure the FBI has not disciplined any individual involved in retaliation against an FBI whistleblower that the Justice Department’s Office of Attorney Recruitment and Management (OARM) found had occurred.¹⁰ According to the letter, individuals responsible for retaliation retired before discipline could be imposed, were found by another office within FBI not to have retaliated against a whistleblower, or had their proposed discipline vacated by the FBI’s Human Resources Division (HRD). I asked you why the FBI had failed to discipline these retaliators, and what message it sends to employees when retaliators are not held accountable. You responded that the FBI “work[s] very hard to try and hold people accountable. Now, often, when people know we’re coming for them, they’ll retire on us and leave government service, which is a challenge.”

⁸ *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (Dec. 2015) (statement of James B. Comey, Jr., Director, Federal Bureau of Investigation).

⁹ *Id.*

¹⁰ Letter from Stephen D. Kelly, Assistant Director, Office of Congressional Affairs, Federal Bureau of Investigation to Charles E. Grassley, Chairman, U.S. Senate Committee on the Judiciary (Dec. 1, 2015).

I agree. But, in most cases involving allegations of retaliation, it is not the retirement of the retaliator that is at issue; rather, it is a failure of the FBI to admit that retaliation had occurred and the failure to impose discipline on retaliators. For the cases FBI provided where the FBI's Office of Professional Responsibility actually found relation or related misconduct, half of the disciplinary decisions were overturned or mitigated. For example, in one instance, OPR found that a supervisor retaliated against an employee who reported a supervisor's earlier misconduct and imposed a seven-day suspension. FBI's Human Resources Division vacated the sentence.

- a. Why has the FBI not imposed discipline against any retaliators during your tenure, and what message does that send to other employees?

You went on to say that "it is not just that enforcement that matters," and you described an award you gave "at the end of the director's awards this year . . . to recognize somebody for blowing the whistle on misconduct. . . . We're an organization dedicated to finding the truth in American life. We have to make sure we're open to seeing the truth about ourselves." "Walking the Talk," as you put it, is indeed critical in fostering a culture within the FBI that is not, as some witnesses said in our hearing on FBI whistleblower protections in March 2015, "hostile to whistleblowers."¹¹ I also agree that recognizing whistleblowers for their contributions is a key element of that effort.

- b. I would like to know more about the award you referenced in your response. According to information obtained by the Committee, that award is a general ethics award that has been given for many years, and was given this year for a report of alleged wrongdoing by other agencies, not wrongdoing within the FBI. Accordingly, please describe the nature of this year's award and the factual circumstances supporting the recipient's receipt of the award.
- c. Please list all of the awards you have provided to FBI employees who reported wrongdoing or other misconduct committed by FBI employees.

12. FBI Investigation Into Matters Relating to Hillary Clinton's Email Arrangement

On March 27, 2015, I sent a letter to the Department of State (Department) inquiring about Secretary Clinton's private server and email arrangement due to concerns that the arrangement interfered with Freedom of Information Act (FOIA) compliance, an issue within the Committee's jurisdiction. The Department has yet to attest that Secretary Clinton's server was approved or certified. Since the March 19 letter, hundreds of emails housed on the server have been deemed to contain classified information, with some information classified at the Top Secret/Sensitive Compartmented Information (TS/SCI) level.

On April 16, 2015, the Department of State Inspector General (State IG) initiated a review of the use of personal communications hardware and software by five Secretaries of State and their immediate staffs. In the course of that review, State IG asked the Intelligence Community

¹¹ *Whistleblower Retaliation at the FBI: Improving Protections and Oversight: Hearing Before the S. Comm. on the Judiciary, 114th Cong. (Mar. 2015) (statement of Michael German).*

Inspector General (IC IG) to validate the procedures being used by the Department FOIA staff as they process 55,000 pages (approximately 30,000 emails) of Secretary Clinton's emails.

According to a June 19, 2015 Congressional Notification from the IC IG, the IC IG reviewed a tranche of 296 of the 30,000 emails Secretary Clinton produced to the Department. The Department had FOIA-processed all 296 emails and released them publicly. After review, the IC IG found two emails out of the 296 that contained classified information – including one email that had been redacted using a “B(1)” FOIA exemption.¹² The other email had been processed and released in an unclassified and unredacted form but should have been marked SECRET//SI//REL USA, FVEY according to officials at the Defense Intelligence Agency, National Geospatial-Intelligence Agency, and National Security Agency. The IC IG notified the National Counterintelligence and Security Center of the release.

On July 6, 2015, the IC IG notified the FBI of the release of the classified information via a Section 811(c) referral, or a “counter-intelligence” referral.¹³ In the referral, the IC IG noted that Secretary Clinton's attorney, David E. Kendall, was in possession of a thumb drive that contained the classified information and was not currently in the government's possession.

On July 23, 2015, the IC IG provided a Congressional Notification referencing additional classified information in potentially hundreds of Secretary Clinton's emails. The IC IG noted that it engaged in a limited sampling of 40 emails that revealed four contained classified IC information that should have been handled at the Secret level. (Congress was formally notified on August 11, 2015 that the intelligence community elements that own the classified information deemed some of the information contained in two emails to be classified at the TS/SCI level at origination.) The IC IG notice further noted that the emails were still, two and a half weeks after the FBI had been notified, on a thumb drive in the possession of Secretary Clinton's personal counsel, Mr. Kendall.

On July 24, 2015, I sent a letter to the FBI asking what steps it had taken to secure and prevent further dissemination of classified information and whether Mr. Kendall had the requisite security clearance to be a lawful custodian of the emails in question. In response, on August 27, 2015, the FBI confirmed receipt of the counter-intelligence referral but refused to confirm or deny any ongoing investigation consistent with “longstanding policy.”

- a. News reports indicate that the FBI acquired Mr. Kendall's thumb drives on August 11, 2015, over one month after the FBI was formally notified via the IC IG's counter-intelligence referral that Mr. Kendall, a private citizen, was in possession of classified government information.¹⁴

¹² 5 U.S.C. 551(b)(1)(A) covers information that is specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy.

¹³ The letter was sent July 6, 2015 by the Intelligence Community Inspector General, I. Charles McCullough, III, to Randall Coleman, Assistant Director, Counterintelligence Division, FBI.

¹⁴ Ken Dilanian, “Clinton relents, gives up possession of private email server,” Associated Press, (August 12, 2015). Available at <http://bigstory.ap.org/article/40f1d5d9d6cc411a83e8466253e6ef3e/us-official-fbi-has-hillary-clinton-emails-home-server>

- i. On what date did the FBI acquire the thumb drives in question?
 - ii. How many thumb drives were seized from Mr. Kendall?
 - iii. What caused the FBI to delay in acquiring the thumb drives?
 - iv. What caused the FBI to eventually seize the thumb drives?
 - v. Did the FBI seize the thumb drive under threat of a search warrant or pursuant to a search warrant?
 - vi. Was the production of the thumb drive by Mr. Kendall voluntary?
 - vii. Is Mr. Kendall, or his law partner Katherine Turner, currently in possession of any of Secretary Clinton's classified emails?
- b. News reports also indicate that the FBI is now in possession of the email server that Secretary Clinton used exclusively for official emails during her tenure.¹⁵ Secretary Clinton has stated that she unilaterally deleted approximately 30,000 emails that she deemed personal. However, the Department of State was not privy to that decision making process, casting doubt on whether all 30,000 were actually personal and raising the possibility that federal records were destroyed.
- i. On what date did the FBI seize Secretary Clinton's server?
 - ii. Did the FBI seize the server under threat of a search warrant or pursuant to a search warrant? Was the production of the server to the FBI voluntary?
 - iii. What caused the FBI to initially seek and eventually seize the server?
 - iv. Has the FBI attempted to retrieve deleted emails from Secretary Clinton's server? If so, has the FBI been successful? If not, why hasn't the FBI attempted to do so?
 - v. Did Secretary Clinton server arrangement include a backup system for storage? If so, were any backup systems located outside of the United States?
- c. News reports indicate that Secretary Clinton's closest advisors, Ms. Abedin, Ms. Mills, and Mr. Reines, each turned over tens of thousands of emails to the Department in September 2015.¹⁶ Has the FBI acquired, or attempted to acquire, those emails? If so, what was the result of that request? If not, why not?
- d. On July 23, 2015, the IC IG provided a Congressional Notification referencing additional classified information in potentially hundreds of Secretary Clinton's emails. The IC IG noted that it engaged in a limited sampling of 40 emails that revealed four contained classified IC information that should have been handled at the Secret level. On July 24, 2015, the IC IG and State IG sent a statement to Congress about the four emails, "These emails were not retroactively classified by the State Department; rather these emails contained classified information when they were generated and, according to IC classification officials, that information remains classified today."

On August 11, 2015, this Committee was notified by the IC IG and State IG that the emails containing TS/SCI material were classified at that level and remain at that level

¹⁵ *Id.*

¹⁶ Stephen Dinan, "Hillary Clinton's aides relinquish more than 100,000 pages of emails," THE WASHINGTON TIMES (September 19, 2015). Available at <http://m.washingtontimes.com/news/2015/sep/19/hillary-clinton-aides-relinquish-more-100000-pages/#>

today. Mr. Kendall and his law partner, Katherine Turner, were allowed to possess the emails from at least December 5, 2014 to August 2015. And in late June/early July 2015, the Department installed a safe at Mr. Kendall's office to store the thumb drive. Given that the emails were that of a Secretary of State, a reasonable person would conclude that they most likely contained highly classified material.

- i. How unusual is it for a government agency to allow a private citizen to store highly classified material in a private law firm?
 - ii. Has the FBI ever allowed a private citizen to store highly classified material in a private law firm? If so, when?
 - iii. Please describe the risk to national security when highly classified information is stored outside of a government facility or SCIF.
 - iv. Due to the fact Mr. Kendall and Ms. Turner had highly classified information in his private office, what steps has the FBI taken, or is taking, to ensure that his possession did not endanger national security?
 - v. Did the Department of State consult with the FBI or other components of the DOJ prior to installing a safe at Mr. Kendall's office? If so, which components, and what instructions and advice were given?
- e. The Department of Justice and FBI have refused to confirm or deny any ongoing investigation consistent with "longstanding policy." However, the DOJ and FBI have publicly acknowledged many investigations in the past. For example, recently the DOJ announced an investigation into the Baltimore Police Department, and the arrest of Ahmed Mohamed, the 14 year old who was arrested for bringing a clock-like device to school that some officials identified as an explosive device. In addition, the FBI recently announced that it is investigating the recent terrorist shooting in San Bernardino, California. And finally, the DOJ announced an investigation into the BP oil spill in the Gulf of Mexico. All these investigations involved very public events, just like the matters relating to Secretary Clinton's server and email arrangement.
- i. Why won't the FBI acknowledge its role, if any, with respect to the potential compromise of classified information or illegal destruction of federal records relating to Secretary Clinton and her associates?
 - ii. Has the FBI used any of its criminal investigative authorities to gather, catalogue, or store information related to Secretary Clinton's non-government email server? Please provide citations to each statute authorizing the FBI's investigative activity on this matter.
 - iii. Is the FBI examining compliance with the Freedom of Information Act?
 - iv. Is the FBI examining compliance with the Federal Records Act?
 - v. Is the FBI examining any matters related to improper destruction of federal records?
 - vi. Is the FBI examining any matter related to the alienation of federal records?

- f. Secretary Clinton exclusively used a private email account and non-government server during her tenure as Secretary. According to interviews with the Judiciary Committee, the Department's Chief Information Office, former Chief Information Office, and former Deputy Chief Information Officer – all who served during Secretary Clinton's tenure – were not aware of the email and server arrangement. In addition, those interviewed could only conclude that Secretary Clinton's server did not have government security protocols in place.
 - i. Was the FBI aware of Secretary Clinton's email and server arrangement during her tenure at State? If so, what security instructions were provided?
 - ii. Given that Secretary Clinton's server did not have government security protocols in place and that highly classified government information was transmitted through and stored on the server, is there a risk that the classified information was compromised by foreign governments? Please explain the basis of your conclusion.
 - iii. Given the classified nature of nearly 1,000 of Secretary Clinton's emails, does the FBI consider an unsecured, non-government server to be a proper place of custody for that information? If so, please explain the basis of your conclusion.

During the hearing, the following exchange took place regarding the FBI's investigation of Secretary Clinton's email and server arrangement:

Senator Cornyn: Does the President get briefings on ongoing investigations by the FBI like this?

Director Comey: No.

Senator Cornyn: So he would have no way of knowing what the status of the FBI investigation is?

Director Comey: Certainly not from briefings from the FBI.

- g. Does Justice Department leadership get briefings on ongoing investigations by the FBI like this? If so, does DOJ, in turn, brief the President on the FBI's inquiry?

Questions for the Record
Senator Orrin G. Hatch
Senate Judiciary Committee
Hearing: "Oversight of the Federal Bureau of Investigation"
December 9, 2015

Questions for Director Comey

1. Over the summer, my staff met with a number of Utah law enforcement leaders to discuss morale and how the current political climate is affecting police efforts. Some of the things these law enforcement leaders told my staff were that:
 - Law enforcement is getting mixed signals about how proactive they should be;
 - The current climate is affecting recruiting;
 - DOJ has been too quick to criticize law enforcement; and
 - People are feeling emboldened to push back against law enforcement.I find these comments deeply troubling. Do you share these concerns? What are you doing to address these concerns?

2. You've spoken several times about the rise in violent crime over the last year in cities all across America. In discussing the reasons for this rise in crime, you've said that you "have a strong sense that some part of the explanation is a chill wind blowing through American law enforcement over the last year. And that wind is surely changing behavior." I've known you for a long time. I've always respected your honesty, and I appreciate your candor on this issue. Please elaborate on your concern about how recent events are impacting law enforcement.

###

NOTE: The Honorable James B. Comey Jr.'s responses to questions for the record are classified and are, therefore, provided separately.

QUESTIONS FOR THE RECORD – Ranking Member Leahy
December 9, 2015 FBI Oversight Hearing

1. The FBI has been reviewing flawed testimony given by FBI analysts on hair comparison analysis in cases prior to 1999. This investigation began in 2012 following the exoneration of three men in Washington, D.C., who were wrongly convicted after FBI analysts gave exaggerated and scientifically inaccurate testimony. In order to review the thousands of cases of potentially innocent defendants, the FBI has been reaching out to the offices that originally prosecuted those cases to get trial transcripts and examine whether the testimony was inaccurate.

On September 14, 2015, FBI Lab Director Christopher Doss wrote in a letter to me and Chairman Grassley that nearly 90 percent of the 3,118 cases that contained a probative association between evidentiary hair and a known sample have been “reviewed or closed.” What troubles me is that the FBI has also said that a case is marked “closed” if the relevant prosecutors’ offices simply ignore the mail and phone requests for information from the FBI. During a briefing on September 15, representatives from the FBI told Judiciary Committee staff that no in-person visits had been conducted to obtain this information because it was “a resource issue.” I, along with Chairman Grassley, have sought clarification on this in multiple letters and have yet to receive a direct response.

There are thousands of defendants, including some on death row, whose cases may have been affected by inaccurate testimony given by FBI analysts. It is imperative that the FBI use every resource necessary to ensure that no innocent defendants remain undiscovered.

- a. If local agencies are not responding to FBI requests for information by phone and mail, the FBI can and must do more. Will you commit to having FBI agents conduct in-person visits to secure whatever documents are necessary to determine whether an error was made in these cases? If yes, what will be your timetable for conducting such visits? If not, why not?
- b. It is irresponsible to close cases without first obtaining the information necessary to determine if a mistake was made. Will you agree to create a new category of cases -- other than “closed” -- for cases in which there has been a lack of response from law enforcement agencies who submitted the cases for analysis? If yes, what will be your timetable for creating this new category? If not, why not?
- c. Will you also agree to actively investigate each of these cases, using all resources necessary, until such information has been obtained or it is determined that the information cannot be accessed?
- d. In how many of the 3,118 cases have you received responses containing the full amount of information necessary to determine whether the forensic testimony was flawed? How many cases have contained errors? How many impacted defendants

have been identified? How many defendants have been notified of mistakes in their cases so far?

- e. The FBI has admitted that 26 of 28 examiners in their microscopic hair comparison unit overstated forensic matches for over two decades to favor the prosecution. Given that innocent people may remain in jail and on death row, why has this investigation not been given higher priority?
2. On March 12, 2015, before the Senate Appropriations Subcommittee on Commerce, Justice and Science, you told Senator Feinstein that the FBI would designate certain cleared individuals to read the full 6,700-page Senate Intelligence Committee Report on the CIA's Detention and Interrogation Program to consider the lessons the FBI should learn to ensure that the mistakes detailed in the report are not repeated. Since that hearing, Senator Feinstein and I have written to you and Attorney General Lynch to urge that appropriately cleared officials from the FBI and the Department of Justice read the full report.
 - a. Have any FBI officials read the full 6,700-page Senate Intelligence Committee Report? If not, please explain why not.
 - b. Have any FBI officials read the executive summary of the report? If not, please explain why not.
3. This year, Planned Parenthood health centers and other women's health clinics across the Nation have experienced a rise in arsons, vandalism, and threats. In September, a Planned Parenthood clinic in Pullman, Washington, was the site of an arson attack. In October, a Planned Parenthood clinic in Claremont, New Hampshire, was damaged by a vandal using a hatchet. And last month, the day after Thanksgiving, a gunman killed three and wounded nine others in an attack at a Planned Parenthood in Colorado Springs, Colorado. I am gravely concerned about the rising numbers of these attacks that terrorize women across this country as they seek health care.
 - a. You testified that investigating access to health clinic violations is one of the "four top priorities" of the FBI's civil rights program. Can you explain the FBI's efforts to investigate threats and attacks against women's health care providers?
 - b. What steps is the FBI taking to prevent such crimes, including investigating extremists who are seeking to prevent women from safely seeking health care at clinics like Planned Parenthood?
4. At the Committee's May 21, 2014, FBI oversight hearing, I asked you about allegations from military commission defense lawyers that FBI agents had interviewed a defense security officer who was part of the legal team representing one of the military commission defendants, and asked him questions about the defense team. These claims raised serious questions about why the FBI appeared to be attempting to recruit a member

of the defense team. You indicated at the hearing that press reports about these allegations may be inaccurate, but you could not comment further because it was a pending matter. However, the FBI's probe was closed earlier this year and no criminal charges were brought.

- a. Now that the FBI's investigation has concluded, please provide a full explanation of the FBI's role in this matter.
 - b. Does FBI policy ever permit agents to attempt to infiltrate the defense team of a criminal defendant, in the military commission system or otherwise?
5. On June 2, 2015, Congress enacted the USA FREEDOM Act. This legislation included a new transitional surveillance authority, sometimes referred to as the "roamer" fix, to allow temporary surveillance in certain circumstances of non-U.S. persons who have entered the United States -- before a FISA court order or emergency authority can be obtained.
 - a. Please describe how the FBI has used this new authority since enactment of the USA FREEDOM Act.
 - b. In your view, is the enactment of this "roamer" fix beneficial to the FBI in protecting national security?
6. As you know, this Committee has taken up the challenge of forging bipartisan legislation to help reform the criminal justice system. Reentry is a key component of the strategy to reduce crime by helping people with criminal records obtain gainful employment and support their families. The FBI has a key role to play in this strategy by ensuring that the results of the millions of FBI background checks for employment and licensing purposes are accurate and up-to-date -- so as not to undermine the employment prospects of thousands of deserving workers.
 - a. How do you respond to the concerns expressed by the GAO and others that the FBI has made only limited progress to improve the accuracy of its employment background checks?
7. In a February 2015 report, GAO noted that the CJIS Advisory Policy Board Disposition Task Force, created in 2009, has still not issued best practices or national standards for collecting and reporting disposition information or developed a national strategy, despite the fact that inaccuracy in background checks continues to be a problem.
 - a. When will the CJIS Advisory Policy Board Disposition Task Force release their guide to advise states on best practices for collecting and reporting disposition information?

8. On September 21, 2015, the FBI responded to a letter from me and Chairman Grassley requesting information on faulty FBI background checks for employment. The FBI's response raised new questions about the agency's limited enforcement of existing regulations requiring states to report dispositions within 120 days and precluding the FBI from reporting non-serious offenses on background checks for employment.
 - a. What more aggressive steps can you take to enforce the existing regulations and update the FBI rap sheets so that workers are not denied employment due to FBI rap sheets that fail to report dismissals and other relevant information about the disposition of the case?
9. The level of reported violence against transgender people this year is deeply alarming. There have been more transgender homicide victims in 2015 than in any other year that advocates have recorded. At least 21 transgender women – nearly all of them women of color – have lost their lives to violence. Last month, the FBI's annual hate crimes statistics report showed that bias-motivated incidents based on gender identity significantly increased from 31 reported in 2013 to 98 in 2014.
 - a. What is the FBI doing to address the growing violence against transgender Americans?
10. According to the FBI's latest hate crimes statistics report, 1,666 jurisdictions reported a bias-motivated incident in 2014. But the vast majority of agencies that submitted data to the FBI (89.2 percent) reported zero hate crimes occurred in their jurisdictions. In October 2015, you rightly said, "We must continue to impress upon our state and local counterparts in every jurisdiction the need to track and report hate crimes. It is not something we can ignore or sweep under the rug."
 - a. Do you believe these numbers reflect an underreporting of hate crimes? If so, what is the FBI doing to address underreporting by state and local law enforcement agencies?
11. A recent report by the Associated Press, "Betrayed by the Badge," recounts alarming stories of law enforcement officers committing acts of sexual violence while on the job. The report includes an examination of cases over six years in 41 states and concludes that more than 1,000 law enforcement officers lost their badges for committing sexual offenses, and this is almost certainly a vast underestimate of actual incidents.

On December 15, 2015, the Department of Justice issued a guidance document entitled "Identifying and Preventing Gender Bias in Law Enforcement Response to Sexual Assault and Domestic Violence." Among the policies urged, DOJ encourages law enforcement agencies to hold officers who commit sexual assault or domestic violence accountable by opening internal investigations whenever an allegation is made, and referring allegations of misconduct to the local prosecutor's office.

- a. How is the FBI working to help implement these policies at the federal, state, and local level? To what extent are you partnering with community-based domestic violence or rape crisis centers or providing technical assistance to state and local law enforcement agencies?
- 12. Intellectual property theft remains a serious threat to American creators, innovators, and consumers. The FBI has long played a central role in protecting these critical economic and cultural resources.
 - a. Please explain the FBI's current efforts to combat intellectual property theft, including information about investigations initiated and/or concluded in Fiscal Year 2015, and any ways in which Congress could further assist you in those efforts.
- 13. The Intellectual Property Enforcement Coordinator is currently in the process of preparing the administration's joint strategic plan to combat intellectual property theft. The plan will draw on public comments and input from relevant federal agencies.
 - a. In your view, what priorities should be included in the joint strategic plan, and what challenges will the administration face in IP enforcement in the coming years?