

FIFTEEN YEARS AFTER 9/11: THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 27, 2016

Available via the World Wide Web: <http://www.fdsys.gov/>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

25-160 PDF

WASHINGTON : 2018

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin *Chairman*

JOHN MCCAIN, Arizona	THOMAS R. CARPER, Delaware
ROB PORTMAN, Ohio	CLAIRE McCASKILL, Missouri
RAND PAUL, Kentucky	JON TESTER, Montana
JAMES LANKFORD, Oklahoma	TAMMY BALDWIN, Wisconsin
MICHAEL B. ENZI, Wyoming	HEIDI HEITKAMP, North Dakota
KELLY AYOTTE, New Hampshire	CORY A. BOOKER, New Jersey
JONI ERNST, Iowa	GARY C. PETERS, Michigan
BEN SASSE, Nebraska	

CHRISTOPHER R. HIXON, *Staff Director*

BROOKE N. ERICSON, *Deputy Chief Counsel for Homeland Security*

DAVID S. LUCKEY, *Director of Homeland Security*

ELIZABETH E. MCWHORTER, *Professional Staff Member*

GABRIELLE A. BATKIN, *Minority Staff Director*

JOHN P. KILVINGTON, *Minority Deputy Staff Director*

STEPHEN R. VIÑA, *Minority Chief Counsel for Homeland Security*

HARLAN C. GEER *Minority Senior Professional Staff Member*

MARIAN P. GIBSON, *Minority U.S. Department of Homeland Security Detailee*

ERIC K. HANSON, *Minority U.S. Army Detailee*

LAURA W. KILBRIDE, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Johnson	1
Senator Carper	2
Senator Paul	15
Senator McCaskill	18
Senator Ayotte	21
Senator Tester	23
Senator Booker	26
Senator Baldwin	28
Senator Portman	30
Senator Sasse	32
Senator Ernst	35
Senator Heitkamp	37
Senator Lankford	39
Senator Peters	48
Prepared statements:	
Senator Johnson	59
Senator Carper	61

WITNESS

TUESDAY, SEPTEMBER 27, 2016

Hon. Jeh C. Johnson, Secretary, U.S. Department of Homeland Security	5
Hon. James B. Comey, Director, Federal Bureau of Investigation, U.S. Department of Justice	6
Hon. Nicholas J. Rasmussen, Director, National Counterterrorism Center, Office of the Director of National Intelligence	8

ALPHABETICAL LIST OF WITNESSES

Comey, Hon. James B.:	
Testimony	6
Prepared statement	73
Johnson, Hon. Jeh C.:	
Testimony	5
Prepared statement	63
Rasmussen, Hon. Nicholas J.:	
Testimony	8
Prepared statement	79

APPENDIX

Information submitted by Senator Carper	85
Information submitted by Senator Booker	88
Statement from Church World Service (CWS)	89
Responses to post-hearing questions for the Record	
Mr. Johnson	90
Mr. Comey	119
Mr. Rasmussen	122

FIFTEEN YEARS AFTER 9/11: THREATS TO THE HOMELAND

TUESDAY, SEPTEMBER 27, 2016

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:02 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Portman, Paul, Lankford, Ayotte, Ernst, Sasse, Carper, McCaskill, Tester, Baldwin, Heitkamp, Booker, and Peters.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing of the Senate Homeland Security and Governmental Affairs Committee (HSGAC) will come to order.

I want to, first, thank our witnesses, Secretary Jeh Johnson, Director James Comey, and Director Nicholas Rasmussen, first of all, for your service to this Nation. The task you face is not easy. I do not envy your task, but I know you all work tirelessly trying to keep this Nation safe. And, we truly do appreciate your efforts.

I will ask unanimous consent (UC) to have my written statement entered into the record¹—without objection—and I will keep my comments pretty short, because I think we, mainly, want to hear from you.

I was in New York, yesterday, as one of the U.S. representatives to the United Nations (UN) General Assembly. And, I had some pretty interesting meetings with Ambassadors, foreign ministers, and other delegations from some of our coalition partners. I think it is fair to say, unfortunately, the general feeling is, America has not led enough to actually accomplish the goal that President Obama laid out 2 years ago, which is to defeat the Islamic State of Iraq and Syria (ISIS).

In June of this year, Central Intelligence Agency (CIA) Director, John Brennan, testified before the Senate Intelligence Committee. And, he said that, unfortunately, despite all of our progress against the Islamic State of Iraq and the Levant (ISIL) on the battlefield and in the financial realm—and we have made progress—“our efforts have not reduced the group’s terrorism capability and global reach.” He went on to say, “They remain a formidable, resilient,

¹ The prepared statement of Senator Johnson appears in the Appendix on page 59.

and largely cohesive enemy.” And, Director Rasmussen, I do not want to steal your thunder, here, but I have to point out that, in your testimony, you, basically, confirm what Director Brennan stated. You say, “It is fair to say that we face more threats, originating in more places and involving more individuals, than we have at any time in the past 15 years.”

But, despite this progress—again, acknowledging the fact that we have made some progress on the battlefield—it is our judgment that ISIL’s ability to carry out terrorist attacks in Syria, Iraq, and abroad has not, to date, been significantly diminished. And, the tempo of ISIL-linked terrorist activity is a reminder of the group’s continued global reach.

Gentlemen, you have a very difficult task: trying to defend our homeland—trying to keep Americans safe. But, in reading this, I just want to make the point that it has been 2 years since President Obama laid out our goal—America’s goal—toward ISIL, which was to defeat it. Two years. It took us about 4 years to defeat Nazi Germany and Imperial Japan. Defeating ISIS on the battlefield, denying them that territory, and destroying that caliphate is the essential first step to reducing those threats that, largely, have not been diminished.

So, again, I thank you for coming here. I appreciate your thoughtful testimony and I am looking forward to your answers to our questions.

With that, I will turn it over to Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman. Let me just talk—I was not planning on getting into this, but, I have a friend, who, if you ask him how he is doing, he always says, “Compared to what?” Well, compared to 2 years ago. Two years ago, ISIS was rolling through Syria and Iraq like Sherman through Georgia. And, 2,000 fighters, from around the world, were going to that part of the world to join up with ISIS—2,000 a month—from the United States, it was 10 a month. Last month, from around the world, 50 showed up. And, from the United States, not even one. We have taken back half, or more, of the land that they had captured from all of the Sunni Triangle. We are moving in on Mosul, which has 2 million people, up to the north—we will take that out next. And, it is not just the United States. This is a coalition. We do not want to have boots on the ground. We made a decision not to have boots on the ground. The American people do not want that.

And, what we do is, we bring intelligence, we bring training, we bring support, and we bring air power. And, together, this coalition is, as we say in Delaware, “kicking”—well, kicking something. And, we are kicking these guys all over Iraq, and we are kicking them around in Syria. We kicked them out of Libya. And, these guys are not 12 feet tall. They are not 12 feet tall. And, we are taking it to them.

What is going on right now? They are losing. They are losing on the battlefield. They are looking for other soft targets. They are looking for other countries to go to, like Libya. And, when they go there, we will take care of them there as well.

So, how are we doing? This coalition is actually doing pretty well. It took awhile to get it together and get it rolling, but we are rolling, now.

But, Mr. Chairman, having said that, I want to thank you for pulling us together, today, on the heels of the terrorist attacks in Minnesota, New Jersey, and New York. Thank you for the hard work and the dedication of law enforcement officials, represented by the folks that are before us today. Those attackers were identified, and they were stopped, before they could fully carry out their plans. And, the vigilance and quick thinking of everyday citizens likely saved many lives as well. That, alone, serves as an important reminder that, if we see something, we need to say something.

While the investigations into these attacks and their specific motives are still being determined, it is clear that these attacks were carried out by two men—two Americans, in fact—who spent most of their lives in our country. These attacks underscore a key fact—the fact that the greatest threat to our homeland does not come from overseas. It does not come from Syrian refugees or from those who travel as tourists on the Visa Waiver Program (VWP). The greatest threat to our country now comes from within—from American citizens and legal residents, who have spent most of their lives in this country—in our country. My colleagues and members of our staffs may recall the words of renowned counterterrorism expert, Peter Bergen, who testified right here, before this Committee, within the past year—last November, in fact—when he said these words: “Every person who has been killed by a jihadi terrorist in this country, since [the attacks on September 11, 2001] (9/11), has been killed by an American citizen or resident.”

Think about that. Many of the attacks are being carried out by Americans—by people who have lived, in some cases, their entire life or much of their life here. They may have come here as children. They grew up knowing nothing else but life in America. Yet, some have suggested that the way to stop these attacks is for America to ban entire groups of people from traveling to our country. Banning entire religious groups from entering the country will not prevent attacks from people—like those committed by Ahmad Rahami, in New York and New Jersey, or Dahir Aden, in Minnesota. Rahami came here at the age of 7, and Aden came here at the age of 2. They grew up as Americans. I believe that those who would seal America’s doors to immigrants and refugees fundamentally misunderstand how to stop these homegrown attacks.

The reality is that stopping homegrown terrorism starts with reaching out to local communities, building stronger partnerships, and making the American dream accessible to all. Fortunately, the Department of Homeland Security (DHS) is doing just that with its Office of Community Partnerships (OCP). I am proud that this Committee passed a bill, with bipartisan support, to enhance the ability of the Department to work with the Muslim community, and others, in order to counter the violent messages of ISIS and other terrorist organizations.

Another important way to battle homegrown terrorism is by neutralizing the terrorists who create the hateful propaganda that is radicalizing our fellow Americans. That is why it is important that we keep taking the fight to ISIS. Simply put, we must continue to

defeat and destroy these guys. And, by doing that, we prevent ISIS from portraying itself as a winner, and we bring to light the horrible abuses it thrusts upon innocent people of every age, race, religion, and nationality. The 60-nation coalition that we lead has put ISIS on the verge of defeat in Iraq and Syria—and in Libya.

For instance, ISIS once held, as I said earlier, a body of land in Iraq and Syria that is about the size of Austria—the size of South Carolina. Over the past 2 years, we have taken a big chunk of it back. We have also taken 45,000 ISIS fighters off of the battlefield, taken out a bunch of their leadership, and cut their funding by more than a third. And, thanks in part to the diligent efforts of our witnesses, we have reduced, dramatically, the number of fighters that are coming to that part of the world.

The other thing that has not gotten much attention is that ISIS is really good at social media. Really good. When they were winning, they were really good at social media. When they were not doing so well, they were doing really well on social media. They are not doing so well on social media anymore—and we have finally learned how to fight that battle and to win that one as well.

I will close with this. This may be Jeh Johnson's last time before this Committee. I just want to take a moment and thank you for your leadership. You remember the old commercial on Oldsmobiles: "This is not your grandfather's Oldsmobile." This is not the Department of Homeland Security you took over—you and Alejandro Mayorkas took over 3 or 4 years ago. You have come a long way—provided great leadership and put together a great leadership team. And, I thank my colleagues for helping to make sure you have had that leadership team, and we have tried to provide adequate funding. And, can you do better? Sure, we can all do better. But, I just want to thank you and Ali Mayorkas, especially, for your enlightened leadership.

I ask that the rest of my statement, Mr. Chairman, be made a part of the record.¹ Thank you.

Chairman JOHNSON. Without objection.

Earlier this month, this Nation marked a terrible day in its history, 9/11, which was an unprecedented attack, on this Nation, by Islamic terrorists. I would just like to have this Committee take a moment of silence, in acknowledgment of that terrible day.

[Moment of silence.]

Thank you.

It is the tradition of this Committee to swear in witnesses, so if you will all rise and raise your right hand. Do you swear the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Secretary JOHNSON. I do.

Mr. COMEY. I do.

Mr. RASMUSSEN. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Secretary Jeh Johnson. Secretary Johnson is the fourth Secretary of the Department of Homeland Security. Prior to leading DHS, Secretary Johnson served as General Counsel (GC) for the Department of Defense (DOD), General Counsel of

¹ The prepared statement of Senator Carper appears in the Appendix on page 61.

the Department of the Air Force, and Assistant U.S. Attorney for the Southern District of New York. Secretary Johnson.

**TESTIMONY OF THE HONORABLE JEH C. JOHNSON,¹
SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY**

Secretary JOHNSON. Thank you, Chairman, Senator Carper, and Senators of this Committee. You have my prepared statement. I will not read it. I will just say, briefly, a couple of things.

One, I have talked, repeatedly, about how we see the global terrorist threat evolving and the threat to our homeland evolving, from terrorist-directed attacks to a global threat environment that now includes terrorist-inspired attacks of the type we have seen most recently, in our homeland, where an actor is self-radicalized, without receiving direct orders from a terrorist organization, and has, as Senator Carper noted, very often spent most of his life here. He can be a U.S. citizen and he can have been born here, but he is inspired by things that he sees on the Internet, social media, and the like.

This makes for a more complicated and challenging homeland security and public safety environment. I think I speak for all three of us when I say that the prospect of the next terrorist-inspired attack, on our homeland, is the thing that keeps us up at night the most often.

Within the Department of Homeland Security, as you have noted, one of the things that I have been very active in promoting is our efforts at building community partnerships, particularly with American Muslim communities. I think, in this environment, it is critical that we do that to encourage them—if you see something, say something. It can make a difference—to build bridges, in terms of grantmaking activity, resources, and the like.

So, this threat is challenging, and it includes not just terrorist-inspired attacks. We now have a new category, which we refer to as “terrorist-enabled attacks,” which is something in between terrorist-directed and terrorist-inspired. And, every once in a while, there is something we refer to as “terrorist-validated,” where a terrorist organization may take credit for something after the attack. And, I am sure we will discuss much of this, today.

As I think you know, I have been very active, lately, in promoting the assistance that my Department can provide to State and local election officials, when it comes to their cybersecurity. In the run-up to the November 8th election, we have been working with State election officials and local election officials, to help them with their cybersecurity, when they ask. I am pleased that 18 States have now come forward and requested our assistance in their cybersecurity efforts.

The last thing I will say is that I am very appreciative of the efforts of this Committee to codify much of what we have done to move forward on my “Unity-of-Effort” initiatives to build, frankly, a better Department of Homeland Security—with fewer stovepipes as well as more efficient, effective hiring and acquisition processes. All of you, I think, are aware of our Joint Task Forces (JTFs) for border security, which is not only a border security mission, but a

¹ The prepared statement of Mr. Johnson appears in the Appendix on page 63.

counternarcotics mission as well. And, I am pleased that the Committees of Congress are seeking to codify that into law. I think that is vital for our homeland security mission, and I appreciate the support for much of our initiatives at management reform. I think you know that the levels of employee satisfaction and morale improved, significantly, this year, thanks to the efforts of our leadership team to get out there and engage the workforce and to show them what we can do to help them with their jobs.

And so, we are building a better, more effective, and more efficient Department of Homeland Security. And, I appreciate the support that we have received from this Committee.

Thank you very much.

Chairman JOHNSON. Thank you, Secretary Johnson. And, we certainly appreciate your efforts.

Our next witness is Director James Comey. Director Comey is the Director of the Federal Bureau of Investigation (FBI). Director Comey has also served as U.S. Attorney for the Southern District of New York, Deputy Attorney General (AG) for the Department of Justice (DOJ), and General Counsel for organizations in the private sector. Director Comey.

TESTIMONY OF THE HONORABLE JAMES B. COMEY,¹ DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. COMEY. Thank you, Mr. Chairman, Senator Carper, and Members of the Committee. It is good to be back before you, again. I should note that this may be the last time I sit next to my old friend Jeh, with whom I served as an Assistant U.S. Attorney in New York many years ago. And, I will miss his presence. I will still be here for another 7 years, Jeh. You are welcome back.

Mr. Chairman, as the Committee knows, counterterrorism remains the FBI's top priority for good reason. What I thought I would do this morning is just, very briefly—in addition to the written statement, which I have submitted in advance—give you a status report on how we think about the most prominent of the threats we face, which comes at us through the group of savages that calls itself “the Islamic State.” I thought I would give you a status report, since we were last together, on the three prongs of that threat.

The first prong is their effort, over the last 2 years, to lure people—troubled souls seeking meaning—to travel to their so-called caliphate. As Senator Carper said, the traveler phenomenon has changed, dramatically, since last summer. It started to go down late last summer, and it has stayed down. Where we used to see 8 or 10 people from the United States, trying to go to the so-called caliphate, we are now down to one—or none—a month. That brand of the caliphate appears to have lost some of its power to attract troubled souls to travel there.

The second dimension of the threat—the second prong—Jeh Johnson mentioned. And, that is, the effort—or the ability—of the so-called “Islamic State” to inspire, enable, and sometimes direct those in the United States to engage in acts of violence. That re-

¹ The prepared statement of Mr. Comey appears in the Appendix on page 73.

mains at the center of the FBI's challenge in confronting this threat. Finding those needles in the haystack—in fact, finding those pieces of hay that might become a needle, and figuring out how to disrupt them before they do harm, is at the center of the FBI's life. It is very hard work, but it is work we aspire to and believe we can do perfectly. And, that is our goal: to do it perfectly day after day after day.

It is a challenge, not just because of the disparate nature of the threat, but because we increasingly are unable to see the communications of those who have become the most dangerous—the phenomenon that we refer to as “going dark.” It is a challenge we continue to try and work around, to mitigate, and to drive a conversation about, in the United States.

The third element of the threat is one we cannot take our eye off of—and I assure you that people at this table and the people we work with have not taken their eyes off of it. The so-called caliphate will be crushed. The challenge will be that, through the fingers of that crush, are going to come hundreds of very dangerous people. They will not all die on the battlefield in Syria and Iraq. There will be a terrorist diaspora, sometime, in the next 2 to 5 years, like we have never seen before. We must prepare ourselves and our allies, especially in Western Europe, to confront that threat, because, when ISIL is reduced to an insurgency and those killers flow out, they will try to come to Western Europe and try to come here to kill innocent people. We have to keep our eye on it and be ready for it. And, I assure you, even though it is not covered a lot, that work is under way every day.

The last thing I will say is that I believe very much that we have changed, as a Nation, and the FBI has changed, as an organization, in the last 15 years. One of the most profound changes in our counterterrorism efforts is our jointness—the way in which we work together—not just at the Federal level, but at the State and local level as well. I think you saw no better example of that than in New York and New Jersey in recent days, where we had everybody surging to a threat and working together in ways that, frankly, would have been unimaginable in 2000, when there was often friction between State and local law enforcement or between Federal authorities across the Hudson River. No more. That is a very important way in which we are transformed. And, it is a testament to the quality of people doing this work. I am proud to be able to represent them.

And so, I appreciate your support of the FBI and our work. I look forward to your questions.

Chairman JOHNSON. Thank you, Director Comey.

Our final witness is Nicholas Rasmussen. Mr. Rasmussen is Director of the National Counterterrorism Center (NCTC). Director Rasmussen previously served as the Deputy Director of NCTC, in various functions on the National Security Council (NSC) staff, and in several key positions with the Department of State (DOS). Director Rasmussen.

**TESTIMONY OF THE HONORABLE NICHOLAS J. RASMUSSEN,¹
DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OF-
FICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

Mr. RASMUSSEN. Chairman Johnson, thank you very much for including me in this conversation, this morning, on our homeland security challenges. And, I appreciate the opportunity also—along with Senator Carper—to discuss the terrorism threats that concern us the most.

As Secretary Johnson and Director Comey have noted, we have had great success. We have made great progress in strengthening our homeland security capacity. And, we have made progress in reducing that external threat from terrorist groups, particularly that threat of a large-scale, catastrophic attack that we faced so acutely on 9/11.

That said, recent attacks in Minnesota, New York, and New Jersey underscore the ongoing threat we face from individuals. This is from individuals who choose relatively simple attack methods and are propagated by terrorist organizations. And, having passed the 15-year mark since 9/11, it is fair to say that the array of terrorist actors, around the globe, that we deal with, today, is broader, wider, and deeper than at any point since 9/11. And, that threat landscape that we face is less predictable than at any point in our post-9/11 history.

ISIL's access to resources, in terms of both manpower and funds, as well as the territorial control that they have enjoyed in areas of Syria and Iraq, those are the ingredients that we have, traditionally, looked to as being critical to a terrorist organization's capacity to mount external attacks. And, for that reason—and this echoes something that Senator Carper said. For that reason, shrinking the size of territory controlled by ISIL and denying the group access to additional manpower—that remains a top priority. And, success in these areas will, ultimately, be essential to our efforts to constrain ISIL's capacity to act as a terrorist group with global reach. And, clearly, significant progress has been made, in these areas—in both of these dimensions.

But, despite this progress, it is our judgment that ISIL's capacity and ability, today, to carry out attacks, in Syria, Iraq, and abroad, has not, thus far, been significantly diminished. And, the tempo of ISIL-linked terrorist attacks and terrorist activity, in Europe and other places around the globe, is a reminder of that global reach.

This external operations capability has been building and entrenching over the past 2 years. And, we do not think that battlefield or territorial losses, alone, will be sufficient to completely degrade the group's terrorism capabilities—necessary, but not sufficient.

Now, the tremendous efforts we are undertaking to counter the ISIL threat are absolutely warranted, but I also want to stress that we still view al-Qaeda, and the various al-Qaeda affiliates, as a primary counterterrorism concern and a top priority. What remains of al-Qaeda's leadership, in the Afghanistan-Pakistan region (AfPak), still aspires to strike the United States and to strike Western interests—although we do not assess that al-Qaeda is capable, right

¹ The prepared statement of Mr. Rasmussen appears in the Appendix on page 79.

now, of an attack on the scale of 9/11. But, that al-Qaeda global network remains dangerous and resilient. And, its affiliates in Africa, the Middle East, and South Asia are focused on developing more connectivity and more unity, despite the pressure they are facing from ISIL.

Al-Qaeda in the Arabian Peninsula (AQAP), in Yemen, and the Nusra Front, in Syria, remain al-Qaeda's largest and highest capacity affiliates. And, they maintain their intent to conduct attacks in the West.

We are, particularly, concerned about al-Qaeda's safe haven in Syria, because we know al-Qaeda is trying to strengthen its global network by relocating some of the remaining leadership from South Asia to Syria—taking advantage of the safe haven. And, as you know, the Nusra Front took steps, in July of this year, to hide its ties to al-Qaeda by changing the group's name and publicly claiming to separate from al-Qaeda. We believe firmly that Nusra Front's disassociation is in name only and that the group remains part of al-Qaeda—supporting the al-Qaeda ideology and focus on attacking the West.

Now, stepping back, there are two concerning trends in the contemporary threat environment that I want to flag. The first, as Director Comey mentioned, is the increasing ability of terrorist actors to communicate with each other outside of our reach with the use of encrypted communications. As a result, collecting precise intelligence on terrorist intentions and the status of specific plots is increasingly difficult.

Second, while we have seen a decrease in the frequency of large-scale, complex plotting efforts that, sometimes, span months or years, we are instead seeing much more rapidly evolving threats, or plot vectors, that emerge quickly or suddenly. And, this so-called "flash-to-bang" ratio—the time between when an individual decides to attack and when an attack actually occurs—the "flash-to-bang" ratio of this kind of plotting is extremely compressed and allows very little time for law enforcement and intelligence officials to get their arms around a plot.

Of course, any hope of enduring security against homegrown violent extremists (HVE) rests in our ability to counter the appeal of terrorism and to dissuade individuals, in the first place. To this end, NCTC continues to refine and expand our work on the prevention side, working closely with Secretary Johnson, his team at DHS, with Director Comey, and with our colleagues at the Department of Justice. This is an area of emphasis for NCTC. It is an area where we can continue to do more countering violent extremism (CVE) and it is an area where we have enjoyed great support from the Committee. And, I look forward to working with the Committee on this issue in the times ahead.

I will stop there, Mr. Chairman. And, I look forward to your questions.

Chairman JOHNSON. Thank you, Director Rasmussen.

This is such an important hearing, that I have decided I will let the questions go for 7 minutes. But, I am going to warn Committee Members that I am not going to let them go a second over that time limit. So, I will be gaveling it. If you ask a question at the

tail end, I will just ask for the answers to be submitted as questions for the record.

Gentlemen, I think it is relatively safe to say that most of your activities involve playing defense. Obviously, some of the intelligence gathering can be used for offensive capabilities, but, by and large, what you are trying to do—and what the Department of Homeland Security, the FBI, and NCTC are doing—we are playing defense.

Now, it is possible you can win a football game by playing defense, if you get really lucky. But, if you are really going to win the game, you have to go on offense.

Director Rasmussen, one of the things I want to talk about is the fact that we have had 2 years where the caliphate continues to exist. And, yes, we have reduced their territory, but, according to your testimony and Director Brennan, we have not reduced their capability. The diaspora has already begun. We are poking a hive and we are doing some damage to it. But, the killer bees are leaving the hive, and they are setting up new hives.

Director Rasmussen, can you talk about what you know of, in terms of the training? We have talked about inspired lone wolves. Now, we are talking about, potentially, ISIL-directed wolf packs—whether it is in airports in Brussels or Istanbul. I have, certainly, heard stories of children, in the caliphate, being trained to do savagery.

By the way, I like your description, Director Comey: “savages” and “barbarians.”

So, Director Rasmussen, can you just talk about what you know, in terms of the effectiveness of their training, both in the caliphate and—as long as they continue to exist—using social media? I think we just witnessed that in New York and New Jersey as well—the pressure cooker bombs—these things that are online. Just talk a little bit about that for me.

Mr. RASMUSSEN. To your question, Mr. Chairman, there was a period, I would certainly argue, at the peak of the caliphate’s geographical expanse, when there was—certainly, a greater share of territory was available for ISIL to conduct this kind of recruitment and training activity. The flow of foreign fighters, which Director Comey referred to, was at its peak approximately a year or 18 months ago. And, at that time, we were, certainly, concerned about the physical space that ISIL owned and the ability of the group to use that physical space to collect these foreign fighters to train, to deploy, to equip, and to create this cadre of potential terrorists, who could be deployed back out to locations around Western Europe and, indeed, around the globe.

That is why the shrinkage of that physical caliphate has been such a high first-order priority of our strategy to defeat ISIL. But, we have acknowledged all along, I think—or, at least, as an intelligence matter, felt all along that there was going to be a lag between the time where we achieved territorial success on the battlefield and the time at which we could actually succeed in constraining ISIL’s ability to carry out attacks overseas. That is because much of that infrastructure that was set into motion or put into place is going to have to be hunted down and destroyed, sys-

tematically. It is not simply a matter of taking territory or winning a battle in a place like Mosul or Raqqa.

So, from an intelligence perspective, it is not that we are at all aiming to minimize the importance of the territorial success that the coalition has had and the shrinkage of the caliphate—not by any means, whatsoever. In fact, destroying the physical manifestation of the caliphate is also a pre-condition for undermining the ISIL narrative—for getting at and exposing the lie behind ISIL’s social media outreach to try to motivate people in the ways that Secretary Johnson and Director Comey talked about.

So, I think of it as a timeline, where the effects we are looking to see are, simply, going to be delayed or lag behind the physical progress on the battlefield. It is not surprising. It puts us in a period of sustained vulnerability that I do not think any of us are comfortable with. But, I think it is a reality.

Chairman JOHNSON. Do you not agree that a year or 2 years from now—and if they still control territory—they still have Raqqa—we will, probably, be making the same statement that we have not reduced their global reach and their terrorist capability, because they have spread—they have set up—whether it is in Libya or some of these other affiliates? I mean, they have to be destroyed. We cannot just nibble around the edges, here.

Mr. RASMUSSEN. If we are sitting here a year from today, I hope we are in a position to say that we have put, considerably, more pressure on that component of ISIL that focuses on external operations—on deploying these operatives overseas—and that we will have done a great deal more work by that time, a year from now, to rip apart that network and to render it less capable.

Will we be at the end of that effort? I do not know that I can predict that.

Chairman JOHNSON. To talk a little bit about the diaspora that, I think, is already occurring—certainly, I am concerned about the potential of ISIL operatives coming into the United States. But, when I take a look at the level of risk—whether it is through refugees, through the Visa Waiver Program, or through an incredibly porous Southern border, I would say that I am most concerned about our porous border. And, Secretary Johnson, I just want to talk a little bit about the latest statistics on unaccompanied alien children (UACs) and family units.

In 2014, we held hearings—and, in the news media, we were talking about this surge—this humanitarian crisis. In 2014, there were 68,000 unaccompanied children that crossed the border. So far, in 2016, we are up to 54,000. In terms of family units, back in 2014, there were about 68,000 family units. We are already at 68,000, with a month to go.

So, we have, certainly, gotten more efficient at apprehending, processing, and dispersing. Let us face it. A lot of them just turn themselves in. My concern is—because we have not stopped the flow or reduced the flow—because we still have enormous incentives for people to come into this country—we have not succeeded in doing that. I am concerned about the diversion of resources on the border—having to take care of what remains, I think, a humanitarian crisis. Again, hats off to your Agencies. The Agencies have gotten better at handling it, but we have not stopped the flow. Can

you just kind of talk about the concern you have, in terms of the Southern border being diverted—still working on these problems?

Secretary JOHNSON. Yes, sir. The underlying “push conditions” in Central America still exist. The poverty and the violence in Central America still exist. In fiscal year (FY) 2015, the numbers of those apprehended on the Southern border went down, considerably. In fiscal year 2014, the total number was about 479,000. And, in fiscal year 2015, it was about 331,000. My projection, for fiscal year 2016, is that we will come in at around 407,000 to 408,000 people apprehended on the Southern border. That is a fraction of what it used to be, but it is still too high.

And, you are correct, Chairman, in that we have gotten better at processing the UACs, in particular, on the front end. We have added resources. But, the “push factors” still exist.

I am concerned about what we refer to as the “special interest alien” that comes from the other hemisphere and who turns up on our Southern border. We do not see this very often. It is a very small percentage of those who are apprehended on our Southern border—people who are coming from the Middle East region. We, now, have in place systems to almost immediately investigate that person, when we apprehend them. I have put in place a working group within my Department, over the last several months, to work with the law enforcement components of other governments, in Central and South America, to interdict these people—before they get to our border—and to share intelligence about what we are seeing. The smuggling organizations that focus on migrants from the Middle East are a relatively limited number. And so, what we are doing—and what I want to do more of—is focus our law enforcement efforts on cooperating with the law enforcement agencies of Central and South American governments, to break these organizations up.

You began your question by referring to migrants from the other hemisphere. And, I think that that is a very legitimate concern—and we are focused on it.

Chairman JOHNSON. Senator Carper.

Senator CARPER. How much time do I have, Mr. Chairman?

Chairman JOHNSON. Seven minutes.

Senator CARPER. Thank you.

I have a couple of “yes” or “no” questions, Secretary Johnson, which I would like to ask you, if I could. Last week, at a hearing in the House of Representatives, there was some confusion about whether the Department’s Office of Community Partnerships is being guided by a strategy. I just want to ask: Does the Office of Community Partnerships have a strategic plan?

Secretary JOHNSON. We have a plan, though—

Senator CARPER. And, my second question is: Can you present that plan to us, say, sometime in the next week?

Secretary JOHNSON. I have given the Office a deadline for giving Congress a plan. I believe that the deadline I gave them was sometime in the month of October. So, you will have that plan in the month of October.

Senator CARPER. All right. Thank you.

Sort of following up on that, one challenge that we face, with stopping homegrown terrorism, is that, as we hear, it is no longer,

solely, a law enforcement matter. We simply cannot arrest our way out of this problem. Stopping homegrown attacks means that we must focus on stopping Americans from becoming violent extremists in the first place—and the Department of Homeland Security's Office of Community Partnerships has taken up the difficult task of building relationships with communities, in order to prevent the recruitment of Americans by terrorists. It is a new Office. It is a new Office with a very tough job. And, with that said, we cannot put all of our eggs in one basket.

This is a question for each of you. We will start with you, Mr. Rasmussen. What are each of your Agencies doing to prevent the recruitment of Americans by terrorist groups, like ISIS? What else can and should we be doing? Everybody realizes—and I love your analogy, Director Comey, about squeezing ISIS—and some of these guys are slipping out through our fingers and going to other places. But, how do we better ensure that they are not successful, as they slip out to other places, including the United States. And, maybe, more importantly, that they are not successfully radicalizing—even from afar—the folks that are here, in the United States? Please.

Mr. RASMUSSEN. Thank you for the question, Senator Carper. NCTC plays two primary roles in our efforts to counter violent extremism—and, particularly, our efforts to prevent terrorist recruitment, particularly of American—U.S. persons. First of all, we provide the analysis that underpins much of the community's effort, trying to understand the process of radicalization, the way in which individuals succumb or find themselves vulnerable to this particular poisonous version of extremist ideology. And so, that analytical understanding helps inform the strategy and policy efforts that Secretary Johnson's task force is leading, at the Department of Homeland Security. So, there is that baseline analytical work that we are doing to support the strategy and policy work.

Beyond that, though, I have officers from NCTC, who are practitioners in this area and are serving on the task force at DHS. We were happy to make our contribution—of our share of the inter-agency kind of quota or tax—of officers to contribute to this effort. I only wish we had more experts that I could send over to Jeh's team to do more. I think this is a capability area that we are trying to grow, inside the Federal Government. We have some really strong expertise. But, I think we need to build more of it—and that starts with my Department, in the first instance.

Senator CARPER. All right. Thank you so much.

Director Comey, the same question.

Mr. COMEY. We have two main responsibilities, in that area. The first, is, obviously, it is our job to try and find those who may be headed in that direction—from consuming poison to acting on it. So, that involves building a complex and very productive set of relationships with communities, teachers, and religious leaders. And then, also, in the online space, making sure we have the sources and the undercovers in place, to see those who might be going from consuming to violence.

Senator CARPER. My sense is, we are doing a lot better in the online space—a lot better.

Mr. COMEY. We are, in one sense. We are not, in another sense. We are making good progress, with the help of companies, like

Twitter, at chasing the “Islamic State,” so-called, off of that space. The challenge is, we have chased them to a place where they are less able to proselytize, broadly, but more able to communicate in a secure way—chased them to applications like Telegram. And so, our mission is to try to get into those spaces, to see what those thugs—those savages—are talking about, in that space. That is our primary responsibility.

But, we are also working with NCTC and DHS. We have a lot of indicators of mobilization to violence, because we have worked, literally, thousands of cases. And so, part of our job is to supply our partners, in the government, the State, and local law enforcement, as well as teachers and religious leaders, with the indicators of someone headed in that direction, so there can be appropriate disruption.

Those are our two responsibilities.

Senator CARPER. Thank you.

Secretary Johnson, the same question. Could you talk further about what the Department of Homeland Security is doing to prevent the recruitment of Americans by terrorist groups, like ISIS? And, what else can and should you be doing—maybe, with our support?

Secretary JOHNSON. We have done a lot, in my judgment, to build bridges, to certain communities in this country, through our engagements, which include the FBI and which include local law enforcement. In my view, where we need to do a lot more is, not only to chase these groups off of the mainline Internet, but also to help Muslim leaders—community leaders—build the countermessage. And so, I would like to see a greater partnership between community leaders and those in the technology sector, who are willing to do this—partner to develop that positive countermessage. It exists at some level, but it needs much greater amplification. I think we are off to a good start.

The other thing I will say is that I am very pleased that Congress, for this fiscal year, gave us some grant money for CVE. It is only \$10 million, which does not go very far. We need to do a lot more of that, in the future. We are going to be making some grant awards, before the end of the calendar year, with that money, but we need more of that. I think that is a critical part of the future.

Senator CARPER. When ISIS was rolling through Iraq, like Sherman through Georgia, they were robbing banks, taking over oil fields, and really building quite a financial presence—quite a treasury. My understanding is that their ability to attract money from those oil operations is greatly diminished. We have, actually, attacked places where they were hoarding actual cash and destroyed it.

It is one thing to defeat ISIS on the battlefield—and we are doing that. It is another thing to engage them on social media. It sounds like we are doing that, I think, fairly effectively.

The other thing that is out there that we have not talked about is: how do we undercut and take away their financial ability—their financial resources to help fund operations around the world—and what are doing in that regard?

Mr. RASMUSSEN. Senator, I think the very way you framed the question highlighted some of the ongoing work we have undertaken to put pressure on ISIL's ability to raise finances. The coalition military campaign has prioritized, all along, the effort to go after ISIL's capacity to exploit Iraq and Syria's oil resources. That becomes a recurring business, because, in many ways, they can reconstitute. Sites are struck. ISIL-affiliated individuals end up with work-arounds, and then they end up being back on the target list, because it is, literally, an ongoing effort.

At the same time, we have also worked with the Iraqi Government to constrain the ability—or the flow of Iraqi Government funds into ISIL-held territories, through payment of salaries and what-not, which the Iraqi Government was engaged in, during some periods of the occupation of major cities. That, again, has shrunk the amount of money available to ISIL.

As you rightly noted, some of the sources of income that ISIL has are now non-recurring. And so, it is a pie that will continue to shrink, over time. But, again, one of the things we have also learned about terrorist organizations is, it does not always take a massive amount of money to fund the terrorist arm of the organization. The resource-intensive bit of ISIL's program was running the caliphate—delivering goods and services to Iraqis and Syrians on the ground, inside of the caliphate. The bit of business that involves deploying operatives overseas or recruiting operatives to send overseas is not, necessarily, the most resource-intensive part of what they do.

Senator CARPER. Thank you very much.

Chairman JOHNSON. Thank you, Senator Carper.

Again, I want to be very respectful. I truly appreciate the fact that we have so many Members here. I want them all to get a chance—giving 7 minutes—so I just ask the Members and the witnesses to watch the clock. If there is a question like that—and both of us ran over. If there is a question at the very end, we will just ask for the answer to be written—just like we do written questions, after the hearing.

With that, it is Senator Paul.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Thank you. One common attribute shared by many of the recent attacks has been that they were previously investigated by the FBI, and they were found not to be credible threats. This would be true of the Boston bombers, the underwear bomber, the Garland, Texas shooter, the Orlando killer, and the most recent New York bomber.

We are all fallible, and I am not here to say, "Gosh, the FBI is terrible, because it missed these things." But, I am also troubled that the FBI is unwilling to even admit that they may have made some mistakes. Every time these come up, what I hear from the FBI is, "Oh, no, we made no mistakes. We did exactly what we should have. And, our conclusion was right, given the information." Well, these are judgment calls, and the judgment calls were incorrect. And so, I think we should at least admit that, and then look at some of the facts.

I am also troubled that the FBI continues to ask for more power, instead of saying, “Well, maybe, we could use our current powers more efficiently and effectively.” And, I will give you, I guess, an example.

Omar Mateen, the Orlando killer, was investigated for a couple years—say we cannot find enough information. Internal policies caused you to end the investigation. There was no law saying that you had to stop it. Maybe, we should talk about whether or not the FBI’s policy should change—about how long you keep an investigation open.

Mateen goes into a gun store. The gun store owner calls you. The FBI shows up. FBI does not get the security footage. Well, I mean, local policemen, in my hometown, know to get the security footage. Everybody does it. That is the first thing you do in any kind of potential crime scene.

Could we not have taken the security footage, matched it with, let us say, how many terrorists live within—terrorist suspects live within 50 miles of that gun store? I do not think we are talking about thousands of people. We might be talking about 20 people. Could we not then present a list and pictures of the 20 people that we have, as suspects, to the gun store owner? Could we not try to match them with the security footage?

We went back for the security footage weeks later, and it had already been erased. Let us admit these were mistakes. I am not even saying that we should hang somebody out to dry. Let us just admit that we are not perfect and we made mistakes, here, because, if we do not admit to mistakes, we are not going to get better.

So, one concern is the length of the investigation. Should we have longer investigations? Are you changing any policy? Or, are you going to tell us, “We made no mistakes, and it is just one of those things?”

And, with regard to opening investigations, I have asked, repeatedly: Why did you not get a warrant? Why did you not do this? Why are you closing the investigation? And, I hear and read that the FBI’s own internal rules say that you have to have probable cause to open an investigation. Well, that sounds to me above and beyond the Constitution. And, I am a stickler for privacy and probable cause. But, to investigate something does not—I would not think it requires probable cause to open an investigation.

So, I think you have all kinds of tools that, maybe, we are not using, adequately. And yet, there seems to be a great deal of lobbying, by the FBI, for new powers: for getting new third-party data, for getting new meta data, for new rules on encryption, for banning technology, and for trying to get involved with technology, when, in reality, I think we need to admit, maybe, there are some problems in our current investigation practices—also acknowledging that we are fallible and that we all make mistakes—and that you cannot be perfect and things will slip through. But, I think to say, “Well, we said these people were not credible threats, but we did not make a mistake. They just were not”—well, they were credible threats, repeatedly. And, when a parent says, “My son is a terrorist”—as a parent, I can tell you that is a pretty hard thing to do—that, maybe, we should try a little harder. The most recent guy

was in jail, and they said, “Well, we did not investigate him. He was in jail.” Well, we never even prosecuted him, which is a whole other criminal justice issue. You do not get prosecuted for stabbing your brother. But, the thing is, if he had a lawyer at the time, you should have at least requested—maybe the lawyer says, “You cannot talk to my client,” but someone should have asked. He gets out of jail after 3 months. He is never prosecuted. Nobody ever follows up.

I think there is a lot of public information you could have looked at. I think there is no reason why you could not open an investigation. And, the standards get much lower when the investigations are opened. The standard for the Foreign Intelligence Surveillance Court (FISA) warrant is not probable cause. It is: “relevant to an investigation.” We can argue about that standard, but that is the current standard. I just do not think we are, necessarily, using our tools adequately. And, I think it is important to admit when we make mistakes, so we can improve our technique. And, I guess, my question to Director Comey is: Is it your position that no mistakes were made, in each of these instances, in judging them not to be credible threats? Would you not have done more to address the situation in the gun store that Mateen went into 6 weeks before the shooting? Would you not have done more—when Rahami was arrested—to question him, because his dad said that he was a terrorist?

Mr. COMEY. Thank you, Senator. Sitting before you is a deeply flawed and fallible human being, who believes very strongly in admitting mistakes when they are made. I hope you saw the very painful moment, when I admitted, publicly, we made a mistake in allowing Charleston, South Carolina shooter, Dylann Roof, to get a gun. So, as long as I am Director of the FBI, we will stare back, very carefully, at what we do. And, where we make mistakes, we will admit them. We will be transparent, and we will get better.

As you know, I hope, I commissioned a lookback at our investigation of the Orlando killer, which is just being completed, now. And, the Inspector General (IG) is going to do another one, which is great, because, if there is learning there, we are going to squeeze it for all of the learning we can get—and get better.

Senator PAUL. But, what is your opinion on the gun store? Should we have done more on the gun store?

Mr. COMEY. Your facts are wrong there.

Senator PAUL. Excuse me?

Mr. COMEY. Your facts are wrong there. The gun owner did not call us contemporaneously. When we were contacted and went back to the store, it was in the weeks afterward, and so the video was not available.

Your facts are also wrong, with respect to what the bomber in New York—who is still alive, and is going to have a trial, I hope, and be sentenced to jail for the rest of his life—so I want to be careful what I say. Your facts are wrong about what his father told the FBI. But, there, as well, we will go back and scrub our prior contact with that matter very carefully—and maybe the Inspector General will as well—which would be great as well. And, if there is the potential for learning, we will learn from it. We are not perfect people. We aspire to be perfect, because we think that is what

the American people have a right to expect. But, you will find us being very candid about our shortcomings and our strengths.

Senator PAUL. With regard to length of investigations and your internal policy on having probable cause to open investigations?

Mr. COMEY. That is just wrong as well. We do not need a probable cause to get a search warrant or to get a wiretap. And, I want to correct something else that you said. You need probable cause to get a FISA warrant from a FISA judge. To open our investigations, the threshold is much lower. We open assessments based on just tips. Then, we open preliminary investigations and full investigations on much lower thresholds, because you investigate to see if there is probable cause.

Senator PAUL. So, should we keep our investigations open longer?

Mr. COMEY. We should keep them open as long as the facts warrant keeping them open—and there is no restriction. As you saw, in Orlando, that preliminary is, normally, set for 6 months. It can be extended another 6 months, and another 6 months, and another 6 months. We have the policies and the tools, by and large, that we need to do this well, which is why we need to look back at each case and say, “So what did we do? Who did we interview? What documents did we get? And, how could we do this better?”

Senator PAUL. But, that would be the judgment call. Should we keep them open longer?

Mr. COMEY. Sure, and that judgment has to be made, every day, by professional agents, with the review of their supervisors.

Chairman JOHNSON. Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you, Mr. Chairman. Thank you all for being here.

I will have a number of questions for the record about bioterrorism funding and BioWatch as well as retaliation in the Transportation Security Administration (TSA). I am very concerned about those issues, especially, since Admiral Neffenger said that there had been no actions taken, in regards to the TSA whistleblower retaliations—and that does not match what has been reported publicly—and I am trying to figure out what the facts are.

I want to spend a few minutes talking about prevention, Director Rasmussen. Prevention is really hard. As somebody who has spent a lot of time in law enforcement, I know it is hard to quantify when you are successful and it is incredibly hard to do it on a performance basis, knowing what is working and what is not. But, I think all of the experts agree that one of the key foundations to the prevention of the radicalization of lone wolves in this country is, in fact, having cooperation and working relationships with the American Muslim community. Would you agree with that assessment, Director Rasmussen?

Mr. RASMUSSEN. Absolutely. And, that is why, what I alluded to, in my response to Senator Carper’s question, is that the officers I have that are working alongside Jeh Johnson’s professionals, in this area, are doing exactly that. They are practitioners, out engaging with Muslim communities around the country, to exactly the ends that you described.

Senator McCASKILL. So, the vilification of the Muslim community, in this country, is very counterproductive to the most essential piece of our prevention efforts to combat the biggest threat we face, which is the radicalization of lone wolves—which is akin to looking for the veritable needle in a haystack. Correct?

Mr. RASMUSSEN. Again, to reiterate, there is no question that we need a cooperative, engaged, and productive partnership with Muslim communities—not just with Muslim communities, but with communities at large, as we deal with the challenge of lone wolves.

Senator McCASKILL. In that light, Director Comey, we have had a number of arsons at mosques across the country. Is there an effort that is beyond—I was an arson prosecutor a long time, so I know about the great work of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). I know about the capabilities we have now, in terms of the technical ability to determine arson. Are you comfortable that all of the resources of the law enforcement community and the Federal Government are being used in a display to the good, patriotic American Muslims, whose places of worship are being burned out of the misplaced prejudice and vilification of a certain religion?

Mr. COMEY. I am.

Senator McCASKILL. And, is there a cooperative effort between both the FBI and the ATF as well as local law enforcement, in that regard?

Mr. COMEY. Yes.

Senator McCASKILL. Is there a team approach?

Mr. COMEY. Yes, we work very well together on those cases and many others.

Senator McCASKILL. Secretary Johnson, when someone, who is on the “terror watchlist” and who believes that they are on the “terror watchlist” erroneously, tries to buy an airline ticket, do they have to, sometimes, miss their flight?

Secretary JOHNSON. I can imagine that happening. Yes, very definitely, ma’am.

Senator McCASKILL. So, it might be that they have to go someplace very important, and they are not allowed to get on an airplane. Correct?

Secretary JOHNSON. Correct.

Senator McCASKILL. But, there is a process that they can then use to get a review of their being on the list. Correct?

Secretary JOHNSON. There is an adjudication process to get off of the list, yes.

Senator McCASKILL. And, approximately how long does that adjudication process take, on average?

Secretary JOHNSON. For the overwhelming majority of cases, where it is a matter of mistaken identity, it is pretty quick. I think it is just a matter of days or weeks.

Senator McCASKILL. But, in the meantime, they have been inconvenienced.

Secretary JOHNSON. Very definitely, yes.

Senator McCASKILL. And, if we had the same process for someone buying a gun, they would be inconvenienced, but, rather than missing a flight to an important meeting or to the funeral of a loved one, they would be missing out on owning a gun for 2 weeks?

Secretary JOHNSON. Correct.

Senator McCASKILL. And, is there any reason that we cannot put into the process a way to add those people to a database that would flag, at the point of purchase, anybody who is on that list—in terms of them being inconvenienced—by delaying their purchase for a few weeks? Is there any reason, either Secretary Johnson or Director Comey—

Secretary JOHNSON. Senator, in my judgment—consistent with the Second Amendment and consistent with a responsible gun owner's right to own a gun, we should give the Attorney General added discretion to deny a gun purchase to somebody who meets certain parameters, similar to the parameters for the “no-fly list” or the “terrorist watchlist.” So, the answer to your question is yes, in my judgment. As a matter of homeland security, I think this is something we need to do.

Senator McCASKILL. Do you think that would be more effective? I mean, I think, after the fact, it is very easy to say that we should start grabbing surveillance tapes in gun shops. Can you imagine the hue and cry if we started grabbing surveillance tapes in gun shops without having probable cause of a crime being committed? I mean, you think the National Rifle Association (NRA) is up in arms about wanting to make sure that we do not inconvenience anyone that is on the “terrorist no-fly list” for a couple of weeks. Can you imagine what the reaction would be, if we started, unilaterally, seizing purchase videos in gun shops? I mean, do you think, Director Comey, that is something that the FBI would even be comfortable doing without probable cause or without some reason to believe a crime has been committed?

Mr. COMEY. We do not seize anything, except pursuant to law. So, we would not be comfortable in doing anything outside of that construct.

Senator McCASKILL. So, I guess the purpose of this line of questioning is, I do not get why we are having a long hearing on the danger of terrorists, in this country, when we cannot even take the baby step of saying that someone, who is going to be inconvenienced by missing a flight, cannot have the same inconvenience for buying an AR-15, which can kill a number of people in a short period of time—even when that person is on the same list. It is, I think, frankly astounding to me. And, I was really pleased to see, last night, that both Presidential candidates agree. So, I am hopeful that the people, who have refused to vote for this, in this body and on this Committee, will take another look at it. Because, I think, we can pound our chests about how long you are investigating people or second-guessing the factual determination that goes into probable cause as well as argue for seizing the videos of gun shops. But, I just do not know how we can, with a straight face, say that we are serious about this, without taking that important step.

I will say that I was in Jordan, looking at the screening procedures. I know that both of you were involved in your Agencies, Director Rasmussen and Director Comey, and I was astounded at how detailed the screening interviews and processes were, on the ground, in Syria. And, I was much more comfortable about that than the Visa Waiver Program. And, I made it. Look. I made it.

Chairman JOHNSON. I certainly appreciate that.

Senator McCASKILL. You did not even have to yell at me.

Chairman JOHNSON. I appreciate it. I will say that the answer to your question is, because terrorists kill people with knives, homemade bombs, and trucks. That is why. Senator Ayotte.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. Thank you, Chairman. I want to thank all of you for your service to the country.

Director COMEY, I wanted to follow up on one of Senator Paul's questions, and start with this, in terms of the Mateen situation, in Orlando. I understand that he was interviewed twice by the FBI, and then the inquiry was closed. Is that true?

Mr. COMEY. Yes. He was interviewed twice during a 10-month or 11-month investigation. Then, the preliminary was closed.

Senator AYOTTE. So, in that investigation, was there any work done to see what he was doing online? In other words, you interviewed him in person. Was there anything looked at, to see what he was doing online?

Mr. COMEY. As I understand it today, there were no search warrants for the content of any of his devices or for the content of his held by a service provider.

Senator AYOTTE. I guess my question is, there is even work you can do without a search warrant—just publicly. Was anything done to see whether he was saying anything online—or doing anything—without going and getting a search warrant, at that point?

Mr. COMEY. In public? Like public postings on social media?

Senator AYOTTE. Public space. Did the FBI do anything?

Mr. COMEY. I do not know the answer. I do not think so, at this point.

Senator AYOTTE. OK. So, one of the things that—as I understand, too, from what I have heard, in prior briefings—that was not done. And, as I look at the situation, one thing that I would assume that we would do, in every investigation—even before we got to the level of looking for content—is to see if there is anything, in the publicly available space, that individuals you are following up on may be saying about terrorism—about any extreme figures. Would you agree that that would be a natural step, in an investigation?

Mr. COMEY. Maybe. And, maybe, that is one of the things we learned from our lookback. It would depend upon the investigation. This one had two sources, who were speaking to him, including taping conversations with him. So, I think the case agent thought they had a pretty good vector into his state of mind.

Senator AYOTTE. Well, I guess my question goes to whether there are lessons learned and whether everything was done well, in Orlando. This one seems obvious to me—that, when you have an individual, who has made some extreme statements—you are interviewing them—we know also that you tried to verify, through secondary means. But, it just seems surprising to me that there was not some kind of online work done, for something so significant. So, that, to me, is of deep concern. I hope you will give us a report of exactly what was done—or not done—in that instance.

One of the things that I know is important to the FBI—because you have testified before other Committees—is wanting the authority—what is called the electronic communications transactional records (ECTR) fix. Can you explain the significance of that, to this Committee—and why it is important? Because, having been a prosecutor before this, I can assure you that, in your basic child pornography case—Internet predator case, I was able to get these types of records. And, tell us how you are being limited, right now—and why you need us to fix it.

Mr. COMEY. Sure. For many years, we were able to issue national security letters (NSL), which were issued in our national security, counterintelligence, or counterterrorism cases for telephonic transaction records and Internet transactions records—not the content of people’s calls or their emails, but the Internet Protocol (IP) addresses involved and who they communicated with on the Internet and by telephone.

Several years ago, lawyers for some Internet service providers started to interpret the statute to say that, if you read the language, it actually—through what I think was a mistake—should not allow you to use a NSL to get transaction records on the Internet, where you can get them on telephone, and interpreted that way. The fix that we think—because we think Congress intended to allow us to use NSLs in both circumstances—is needed is to allow us to get non-content for telephone transaction records and Internet transaction records.

Senator AYOTTE. And, you would agree that this is a very common tool in criminal cases—just average criminal cases—where you are not getting content, but you are, actually, in many instances, issuing a subpoena to get the basic electronic records. And, it seems absurd to me that we cannot make that basic fix that only failed the Senate by one vote. So, I hope we can get you that authority.

I wanted to also follow up on the most recent case, where Mr. Rahami has been arrested. And, in that instance—I know Senator Paul had asked you about that, but one thing is—what the public reports of what is out there. It is my understanding that he was actually flagged by the Department of Homeland Security after he arrived back from Pakistan—and notified by the National Targeting Center (NTC), based on when he was stopped at the airport. And, the National Targeting Center, as I understand it, is under the Department of Homeland Security, specifically, U.S. Customs and Border Protection (CBP). And, as a result of that, that information was passed on to the FBI.

Later, in August 2014, Mr. Rahami’s father makes some type of report of some connection to terrorism. And, at that point, that was also provided to the FBI. So, the reports are that he was never interviewed there.

So, what I think we are trying to understand is, these are basic steps that, when you have someone traveling to Quetta, Pakistan—even if they have family members there—we know that is a hub of terrorism and a very dangerous place. And, that flag—and that travel history, combined, later, with a report, where a family member may have reported a potential tie with terrorism—and yet, there was not an in-person interview.

So, can you help us understand? Do you have enough people? Is there some reason why he would not be interviewed? And, what are the things we need to learn from this? Because, obviously, we want to prevent it, in the first place. But, when something like this comes through your doors, we want to make sure it is followed up on, so that we can do all we can, with local law enforcement, to stop these things before they start.

Mr. COMEY. Thank you, Senator. I will, at some point, want to have that conversation. I do not want to have it, now, for two reasons.

First, this is an active investigation. This guy is alive and entitled to a fair trial. And, I do not want to do anything that gives him an opportunity to claim we deprived him of that right.

And, second, I do not know yet. We are going to go back and look, very carefully, at the way we encountered him. And, we will find the appropriate forum to be transparent about what we did well, what we could have done better, and what we have learned from it. We have not done that work yet, because we are doing an active investigation. So, I do not want to comment in this forum, beyond that, right now.

Senator AYOTTE. Well, I appreciate that. But, I think this is a really important question for all of us. First, do you need different legal authorities? Second, do you need more agents? Third, was it a case of something being missed, that this individual was not interviewed, despite these flags? If we look at the Orlando situation and if we go back to the Boston Marathon bombers, Tsarnaev brothers—each one of them—putting them together—what more do we need to do? What are the lessons learned? And, if you need additional support, we need to know about it very quickly.

Thank you.

Chairman JOHNSON. Senator Tester.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman. I want to thank each one of you for being here, today. And, thank you for the work you do. And, a special thank you to you, Jeh, since this is your last time in front of this Committee.

Jeh, you brought up support for State governments on election tampering. Could you give me an idea on how prevalent this is by foreign governments?

Secretary JOHNSON. We are seeing a limited number of instances, where there have been efforts, through cyber intrusions, to get into the online presence of various State election agencies. And, one or two of them have been successful—others have not. But, more broadly, just in the general environment, Senator, that we are in, where we have an increasing level of sophistication with nation-state actors, “hactivists,” and so forth, we have been out there saying to State election officials, “If you need help, just ask us for it.”

Senator TESTER. So, they are getting into the databases and changing the votes? That is what they are doing?

Secretary JOHNSON. No. No, that is not it. The matters are under active investigation. I think there is a limited amount we can say.

Senator TESTER. OK.

Secretary JOHNSON. But, what we are seeing are efforts to get into voter registration rolls and get the identity of registered voters—things of that nature—not to change a ballot count.

Senator TESTER. OK. And, change votes—

Secretary JOHNSON. Not to change votes, no.

Senator TESTER. No, but to change it, so a person, who would normally be registered, would not be registered, then? Is that what we are talking about? Or, to register people who are not registered?

Secretary JOHNSON. I cannot say that.

Senator TESTER. OK.

Secretary JOHNSON. No, I cannot say that.

Senator TESTER. Alright. And, is this coming from one particular country?

Secretary JOHNSON. I do not believe that we have reached a determination of that nature, to that extent.

Senator TESTER. OK. We talk about the Southern border a lot. I always talk about the Northern border.

Secretary JOHNSON. Yes, you do.

Senator TESTER. And, I want to talk about that, for a second, in the arena of communications. We have been told, by folks who work under you, on the ground, on the Northern border, that there are gaps in communication on the Northern border. Are you aware of those gaps? First, are you aware of those gaps in communication? Do they exist?

Secretary JOHNSON. It is something that I have heard about, and I know you have an interest in this. Frankly, I would not be surprised if there were some level of gaps in communication that should not exist.

Senator TESTER. Right. And, I guess the next question is, then: If you do have gaps—which is not unreasonable, but it is something we need to work on, though, to get it fixed—do you have work-arounds on those gaps, through local law enforcement, highway patrol, or municipal sheriff departments—whatever it might be?

Secretary JOHNSON. I would have to get back to you on that, Senator.

Senator TESTER. Could you check on that? Because I think that that is—if we have dead zones on the Northern border, that is a particular problem and a concern that, quite frankly, is pretty basic. And, if you could find out and just let me know, that would be great.

Secretary JOHNSON. Sure.

Senator TESTER. I want to talk a little bit—since this is your last meeting, Jeh—about DHS. DHS is a behemoth of an Agency. It is massive, and you have done a masterful job, in your job, there. I think you report to a number of Committees. I think, maybe, 119 Congressional Committees and Subcommittees—119.

Secretary JOHNSON. Depending on how you count, yes, sir. [Laughter.]

Senator TESTER. Yes. Well, I count in base 7, so there may be less than that. Or, there may be more.

Secretary JOHNSON. I love Congress.

Senator TESTER. Do you have any ideas—I mean, I cannot imagine—first, from an accountability standpoint, it does not make

much sense to me, because, how can this work? And, second, do you have any actions that you think Congress could do, on your way out, that would make you all more accountable and, quite frankly, more functional?

Secretary JOHNSON. Well, first, we have, actually—notwithstanding the number of Committees and Subcommittees—we have actually reduced the amount of time it takes to respond to a Congressional inquiry, pretty significantly, since I have been Secretary. And, we do spend a lot of time responding to requests. I will say that I read every letter from a Member of Congress that comes in. About half of them are from the same two people. No names mentioned, here.

Senator SASSE. You are welcome.

Chairman JOHNSON. It is called oversight.

Secretary JOHNSON. You are not one of the two. No, sir. [Laughter.]

The real problem with having so many Committees—being divvied up among so many Committees, it is very tough to get any kind of comprehensive authorization of our activities through Congress. That is the real substantive problem with having so many Committees of oversight.

Senator TESTER. Is there a solution to that? Should we just give it to this one and be done with it?

Secretary JOHNSON. I would say—look, in a perfect world, I would say that there should be one oversight Committee for authorization and one Committee for appropriations—just like in my Department of Defense days. We had the Senate Armed Services Committee (SASC) and we had the Senate Appropriations Committee—and that was it. And, if I appeared before any other Committee, I got in big trouble.

Senator TESTER. OK. And, this is for both you and for Jim Comey. Canada has changed its policy for Mexicans traveling up to Canada. And, there is not much we can do about that. It is between those two countries. But, this policy—and I think I sent you a letter on it. In fact, I know I sent you a letter on it. And, I think you responded to it, and I appreciate that you read it. Has this changed our posture at all toward the Northern border, because of the potential appearance of loosening travel restrictions?

Secretary JOHNSON. It depends on how they arrive into Canada. If it is by air, that is one thing. If it is on land, that is another.

I will say that we are building information-sharing agreements with the Government of Canada, so that we have a better sense for who is coming and going across our border into Canada. And, I think we need to keep moving in that direction.

Senator TESTER. OK. The last thing, because it has been claimed here a couple times—do you see yourselves as only playing defense?

Secretary JOHNSON. That is an interesting question. When I was at DOD, signing off on a lot of targeted lethal force, as consistent with law, I suppose I was on offense. I think it is inherent, in the DHS mission, that we are on defense. But, I think it is also incumbent upon us to have an affirmative agenda for improving our mission and for how we do business. So, I have tried to do both.

Senator TESTER. Thank you all.

Thank you, Mr. Chairman.
Chairman JOHNSON. Senator Booker.

OPENING STATEMENT OF SENATOR BOOKER

Senator BOOKER. Thank you, Mr. Chairman.

First and foremost, I just want to thank you all for your work. It is incredible, the dedication you all have. You are truly patriots to our country. And, obviously, what we all witnessed happening, in New Jersey and New York this past week, is a further affirmation of the quality of your commitment to the security of our homeland. And, I appreciate you saying earlier, Director Comey and Secretary Johnson, that this is a multiple-level commitment from local authorities as well as from State and Federal authorities, because, what we saw, the commitment amongst the Linden, New Jersey police officers, for example, who, literally, took fire from a terrorist—saved lives—I reached out to the two gentlemen last week. And, there is truly heroic work being done at every level of our government.

Secretary Johnson, I have been very concerned and focused on issues of rail security. It is something that I feel we are not doing enough about, especially given the Northeast corridor. More people travel along the Northeast corridor, by rail, than they do on air travel. We have seen that the pipe bombs found in the Elizabeth, New Jersey train station were near Amtrak—New Jersey Transit, where millions of people ride, in the State of New Jersey.

In 2007, Congress actually passed legislation requiring that TSA and other Agencies implement a number of recommendations that came out of the (9/11 Commission). Among them were several requirements for TSA to issue regulations that would provide direction to public transportation agencies, railroads, and bus companies on security training for frontline transportation workers.

Since the passage of the legislation, there have been several critical events, from the Brussels metro bombing to, more recently—again, what we saw in New York and New Jersey—near train stations. And, if you look at it from a larger perspective, since 2001, there have been more than 1,900 attacks that have been carried out against transit systems, globally—resulting in thousands of deaths—about 4,000—and 14,000 injuries.

However, TSA, currently, has less than 800 full-time employees dedicated to protecting surface transportation assets, which is less than 2 percent of the Agency's workforce. If you just look at the proportion of what we are applying to air travel compared to surface travel, you see it is almost as if we are still fighting the 9/11 efforts and not really looking forward to what the attacks are that we are seeing, consistently, around the globe, today.

I have been discussing this, with TSA status—have been writing letters about it. I hope I am not in your top two, but I definitely have been pushing this for some time. And, frankly, it is just becoming very frustrating to me.

And so, I just want to ask very specifically: Can you please provide me with a very specific timeline on when TSA is going to finish its work on the 9/11 Commission's recommendations, Secretary Johnson?

Secretary JOHNSON. Yes, we can get you that timeline.

Beyond that, I will say that I am also a regular user of the Northeast corridor and of New Jersey Transit. And so, I am very familiar with rail security. Frankly, I believe that TSA's principal focus should continue to be aviation security, given the threat streams that we all see. That needs to be their number one priority. They do have the rail security mission as well, but, as you know, Senator, we have Amtrak police and New Jersey Transit police to support that mission as well. But, I would like to see us continue to develop that aspect of TSA's mission, so that we are in a better place.

Senator BOOKER. I appreciate that, and I appreciate your commitment to get me a timeline. This is an issue of proportionality—2 percent going to surface transparency and 90-plus percent going to aviation. At least in terms of proportionality, does it seem a little out of whack?

Secretary JOHNSON. I would want to think about that a little bit more. Again, when it comes to rail security, we have other security forces out there supporting the mission. So, I would want to think about whether that is the right ratio or not. I continue to be concerned about aviation and airport security—and I believe that needs to be TSA's principal focus.

Senator BOOKER. And, I am not arguing with that. Again, I look forward to getting the timeline.

And, just really quickly, Director Rasmussen and Director Comey, do you believe that Rahami was part of a cell of other terrorists that were planning attacks?

Mr. COMEY. That investigation, as I said earlier, is open. We see, so far, no indication of a larger cell or the threat of related attacks.

Senator BOOKER. And, it is interesting that you are seeing a spiking of violent extremism happening. Secretary Johnson—I appreciated his talk about the terrorist diaspora, like has never been seen before, as we win on the ground—continue to win on the ground in Syria and Iraq. Can you give me sort of more of an idea of why you think there is a spike going on? And, what are some of the root causes of this?

Mr. COMEY. For me, Senator?

Senator BOOKER. Yes—either one.

Mr. COMEY. Well, at least what I was talking about, in terms of the terrorist diaspora, is, we know thousands—tens of thousands, by some measures—of fighters have flocked to the so-called caliphate. Many have died in battle there—and many more will die, as the caliphate is crushed. What I am talking about is the future that we have to focus on—

Senator BOOKER. So, can you just hone in on 2015. There has been a spike, right? And so, this is not, necessarily, a result of the gains that we are making in Syria and Iraq. Do you have another understanding of why we are seeing a spike in 2015, and, seemingly, in 2016 as well?

Mr. COMEY. Well, we saw a spike, in the United States, of people moving toward violence, because ISIL started investing in their social media campaign, in 2014. It paid dividends, starting in the spring of 2015, where troubled souls started to flock to it, electronically—and be motivated to move to violence. We have made progress against that—against locking those people up—and dis-

rupting some of that narrative. And so, the numbers have come down, slightly.

Senator BOOKER. Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Baldwin.

OPENING STATEMENT OF SENATOR BALDWIN

Senator BALDWIN. Thank you, Mr. Chairman.

I also want to explore the—well, first of all, thank you for being here—appearing today—and for your work. I want to continue to explore what you talked about, Director Comey, with regard to sort of the impending terrorist diaspora, when the caliphate is crushed. In your testimony before us this morning, you talked about the fact that this is not an often-looked-at area, but that work is under way—and you assured us of that.

I guess I would ask you and Director Rasmussen about, sort of what your early estimates are, of what that is going to look like, globally, and sort of the “where, when, and who.” I understand the things that are dependent—that we have to know, first, when we consider action on the ground to be concluded.

But, I would like to hear what your early estimates are. And then, what sort of strategic changes we should look toward, domestically. What is going to be the impact of that diaspora, domestically? What sort of policy and resource implications does that have?

So, realizing that we are not in a classified setting, tell us what you can about that work under way.

Mr. COMEY. Certainly, Senator. And then, Nick will both check me, and probably make the answer more thoughtful. But, I will take the first shot.

Certainly, at least hundreds of fighters are not going to die in the coming crushing of the caliphate. The caliphate, as Nick Rasmussen has said and as Secretary Johnson has said, has been steadily losing territory. There is going to come a point, where it is going to be, essentially, crushed. I do not know exactly how to estimate that, over the next couple of years. Through the fingers of that crush are going to come some very bad people—a much larger diaspora than we saw, for example, out of Afghanistan after the mujahideen—the conflict with the Soviets that ended in the late 1980s.

And so, the most important way to prepare for that is to knit ourselves together, especially with our European colleagues, because most of that flow is going to go up into Europe, from which it came. And so, there is a tremendous amount of work under way, including by the FBI, in making sure people are taking advantage of the data we have gathered, both in our Terrorist Screening Center (TSC) and in our investigations—and connecting themselves to us and, maybe, most importantly, getting our European colleagues to learn the lessons we learned, after 3,000 people were murdered in our country, 15 years ago—where we broke down the barriers and knitted ourselves together.

Our European Union (EU) colleagues must do that—and connect themselves to us and our information better, so that we can spot and disrupt that flow when it comes.

Senator BALDWIN. I know my time is going to be very limited. What I will want to get to, fairly quickly, is the domestic implica-

tions and the planning under way for how we pivot, from looking for that needle in the haystack—the lone wolf—the radicalized person, to those who may gain access to the United States in this diaspora—maybe, well identified in advance. So, if you could—

Mr. COMEY. I will do 30 more seconds. Then, I will let Director Rasmussen follow up.

In a sense, that is the threat we have been preparing for since 9/11: the external flow of terrorists looking to come into our country. That is where we have made such tremendous progress. So, to my mind, it is simply about continuing to do what we have done well, and finding ways to improve that. But, really, the central part of that mission is getting our partners, outside of the United States, to learn the lessons and to travel the journey we have traveled, in 15 years—and do it much more quickly. Nick.

Mr. RASMUSSEN. I just have a couple of points to amplify the Director's comments, because I think what he is pointing to is exactly right. What we have succeeded in doing, across both Administrations, over the last 15 years, is creating an end-to-end watchlisting system that allows us to have confidence that, if we have an identity, we are very likely able to prevent an individual from getting into the United States.

The problem is, as the Director said—and, actually, there is a good-news story there in that, I think, terrorist organizations look at us as a harder target, as a result. They know it is harder for individuals to get into the United States than it is to get into Western Europe or, certainly, into other parts of the world.

But, the problem is, we are not our own ecosystem, as the Director said. We are dependent, in part, on what our partners share with us, in terms of the information they have. We are, probably, the most aggressive collectors of identity information about terrorists—or potential terrorists—of any country in the world, but we cannot capture it all. And so, what we can get from our partners will give us the tools to identify someone at the border, to put them on a watchlist, and to make sure they cannot enter the country.

I would point to one last challenge on this, and that is that, even as good as we are at this and as much progress as we have made in creating this end-to-end system, it is still a name-based system. And, over time, it needs to transition to a biometrics-based system, because terrorists, over time, have shown that they have the capacity to innovate, and they can develop the kinds of documents that, over time, might be able to fool us. And so, I think we would all be more comfortable if, a decade from now, we had a biometrics-based capacity to identify travelers at the border—or potential terrorists—rather than a name-based system.

Senator BALDWIN. Thank you for those answers. I have a minute left. And so, I am not sure I am going to get the whole answer on the record, but let me present the question. I am trying to bring this, from this impending diaspora, to sort of the domestic implications.

Secretary Johnson, I wanted to just highlight something that is concerning me, in my home State. And, that is the availability of grant resources for local partners. So, in the largest population center of our State, the surrounding Milwaukee area—their fusion center, the Southeastern Wisconsin Threat Analysis Center, recently,

actually, worked with the FBI to thwart a terrorist attack in that city.

Unfortunately, they have had to reduce their full-time personnel by two-thirds when Milwaukee no longer qualified for the Urban Area Security Initiative (UASI) funding—under the risk formula. And, I know that they could use additional funds.

So, given the increase in attacks on soft targets, across the country, would you agree that there is a need for increased grant funding? And, can you report back—again, we are not going to have time for your answer on the record—on the threat portion of the formula evolving, in light of the uptick in soft targets?

Chairman JOHNSON. And, the Secretary can respond in writing on that.

Secretary JOHNSON. Yes.

Chairman JOHNSON. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you to all three of you. You guys are helping, every day, to keep our country safe—and no one is infallible, nor is our system—as we have seen, because there have been gaps and there have been problems. But, we want to thank you for your service, today.

I am, particularly, concerned about two things. One is the home-grown terrorist threat. We have talked about that before, on this Committee and in our Subcommittee—and I continue to believe that our online presence is not what it ought to be, particularly, the counternarrative. I understand these groups are moving away from some of the services, like Twitter, which is good, but they are going to encrypted sites, as Director Comey said. And, we still are not figuring out who has responsibility for that. And, I want to get into another topic, so I will not ask you to respond to that. But, I may ask you some questions—more detailed questions—in writing, regarding who is in charge and how we are going to get the best minds working on the counternarrative to counter what we are seeing online, which, even today, continues to attract some of our young people. Before this Committee, you told us, a few months ago, you were concerned about this issue. When you are talking about foreign fighters and other jihadists scattering, in 2 to 5 years, as you have said this morning—that being one of your major concerns—you have also told us that we have gaps in intelligence there, particularly, in what you call the “crucial zones of conflict.” So, to me, this is a critical issue. And, it was just raised by one of my colleagues. But, how do you get that intelligence, so that, when people are scattering—and, Director Rasmussen, you talked about the need for biometrics, because of people being able to change their identity, as we have seen in the European situation. Those are the two concerns that I think are the most pressing for me.

But, if I could raise another issue, since it is a 9/11 hearing, there is legislation that we have worked on—thank you to Secretary Johnson for bringing it to us. The Federal Emergency Management Agency (FEMA) wants us, very much, to codify and help protect some of our urban search and rescue volunteers. FEMA task forces, around the country, rely on firefighters and other ex-

perts to come together and form these task forces. We are really proud of our task forces in Ohio.

And so, we wrote legislation, which was reported out of this Committee, unanimously, on May 25th, with the support of FEMA and the Administration. Ranking Member Carper is a cosponsor and Senator Booker is a cosponsor. They have both agreed to try to help to get this thing done.

We have now had it on the floor for a while, with no success getting what is called a "hotline" done—meaning just getting everyone to approve it, since it is non-controversial.

So, I am just announcing, today, that I plan to go on the floor and offer it under unanimous consent, because we cannot figure out who is blocking it. We cannot imagine someone would want to block this.

On 9/11, I was here. My wife was visiting—a rare visit to Washington, actually—and 9/11 hit. She got what I think was the last rental car out of Enterprise, out of Washington, and drove straight home to be with our kids. And, as she was driving, on some lonely highway, in Pennsylvania, Ohio Task Force One was coming the other way. And, lights were flashing, and she recognized them. And, they were driving into danger. And, I have known a lot of the men and women involved with that task force, including men who went that day, on that trip, who did go into harm's way. They deserve this protection. This protects their job when they get back. It protects them from liability. It protects them, in terms of their insurance. It is just commonsense stuff.

So, one, I want to thank the International Association of Fire Fighters (IAFF). I want to thank FEMA, and others, who have endorsed this, supported this, and helped us to move it. But, let us get this done. We cannot wait until another Congress. FEMA actually came, originally, to this Congress, about 10 years ago, on this issue, and said that they wanted to codify it. So, Secretary Johnson, thank you for your support of it. And, I hope that we can move it forward.

Do you have any comments on that, Secretary Johnson, this morning?

Secretary JOHNSON. Senator, I am familiar with the legislation. I know FEMA is very supportive of it, and I hope it passes.

Senator PORTMAN. Thank you.

With regard to the other two topics, on homegrown terrorism and the online challenge, can we dig a little deeper, as to who is responsible, in our government, to provide that counternarrative? It is not, necessarily, something that government does well, but we, on this Committee, have been able to look at some of the videos that these jihadists and murderers are putting out there, showing terrorists providing candy to children—being in playgrounds—and that it is, somehow, a euphoric life. And then, we have seen some of the counternarrative—and some of it has not been very effective, to be frank. I do not know who is best to respond to that. I know you have been involved with this, Secretary Johnson, but who is responsible, within our government? And, how can we ensure that we can get the best minds, including those from the private sector, involved in this in order to have a more effective counternarrative out there, to stop some of this homegrown terrorism? Which—if you

look at these cases, whether it is Orlando, San Bernardino, or Cincinnati, Ohio, where we had a young man arrested, so much of it is being encouraged by online messaging by ISIS and other groups.

Secretary JOHNSON. Well, first, the countermesssage—just given the nature of it—would not be very credible if it were a government message. This is something that has to be developed within the community.

To the extent that we, in government, have a role in promoting that, facilitating the partnerships, and getting the right people together in the room to develop this countermeasure, we have, in my Department, the Office of Community Partnerships, which, at the moment, is leading an interagency task force that consists of FBI, NCTC, and others, where we draw, from all of our Agencies, the best talent and the best minds. This task force was put together, probably, about a year ago. I think it is a good thing. No one Department has a corner on this, but, there is, in fact, a task force, led by my Department, devoted to countering violent extremism and building community partnerships, which includes this effort to amplify the countermesssage.

Senator PORTMAN. Have you seen their work?

Secretary JOHNSON. I have. I have seen the work that is out there online. I think it needs to have a broader message.

We are also, by the way, encouraging this, through grants—through State Department grants. In the future, I want to see more of my Department do the same thing. We are encouraging young people to develop these kinds of materials, and we are encouraging innovation in this area. But, inherently, it is not a government message.

Senator PORTMAN. I understand what you are saying, about a government message not being as effective. I also, though, believe that we cannot just allow there to not be a countermesssage out there, because the government does not organize it. In other words, if the private sector is not doing it, if you cannot get, as you say, young people to go online, voluntarily, with their own countermesssage that is effective, I think it is incredibly important. And so, we will follow up again, with more specific questions. But, I think the task force—as I understand it, some of the task force efforts have not been very compelling, from a sort of production point of view—to make it so that it is something that can help to change minds and persuade young people. So, we will continue to follow up on that.

Senator PORTMAN. Thank you.

Chairman JOHNSON. Senator Sasse.

OPENING STATEMENT OF SENATOR SASSE

Senator SASSE. Thank you, Chairman.

Director Comey, why was Cheryl Mills granted immunity in the classified data investigation for Secretary of State Clinton?

Mr. COMEY. The Department of Justice wrote a letter to Cheryl Mills' lawyer that gave her what is called "active production immunity", for the production of her laptop. So, it is not personal immunity, for her. The immunity ensures that we, the Department of Justice, will not directly use against you anything we recover on this laptop. It is a fairly common tool in criminal investigations,

but that is what it was. And, the FBI judgment was: We need to get to that laptop. We need to see what it is. This investigation has been going on for a year, and this was, in the negotiation, a tool that her lawyer asked for, which the Department of Justice granted, so we could get the laptop.

Senator SASSE. Thank you. Was she then Secretary Clinton's lawyer, in Secretary Clinton's interview with you? And, is that irregular?

Mr. COMEY. Our understanding was, she was acting as a member of her legal team—not irregular. It is not the FBI's job to decide who can be in a voluntary interview. There are ethical canons that govern lawyers, but we do not police that. If it was a judicial proceeding, the judge might police who could be there representing an individual. But, that is not something that we could do anything about, in a voluntary interview.

Senator SASSE. Secretary Clinton has summarized, to the public, that you have said that her statements in her interview and her statements to the public were truthful. Do you think that is accurate?

Mr. COMEY. As an investigator, I kind of look at the world in an odd way. I never say that I believe anybody or that anything is truthful. I always ask: Do I have evidence to establish that it is untruthful or that I do not believe somebody? And so, as I said, when I testified about this, for 5 hours, in July, we did not develop evidence that led us to believe that any of the statements to us were untruthful.

Senator SASSE. Do you think that Cheryl Mills would have destroyed her laptop? And, if so, why was there this negotiation, as opposed to just asking for it by a grand jury subpoena?

Mr. COMEY. Well, it is a lawyer's laptop. So, having done this for many years, a grand jury subpoena, for a lawyer's laptop, would likely entangle us in litigation over privilege for a very long time. And so, by June of this year, I wanted that laptop. Our investigators wanted that laptop. And, the best way to get it was through negotiation.

Senator SASSE. Do you think any laws were broken by Cheryl Mills?

Mr. COMEY. We have no evidence to establish that she committed a crime.

Senator SASSE. Do you think that Secretary Clinton broke any laws, related to classified data?

Mr. COMEY. We have no evidence sufficient to justify a conclusion that she violated any of the statutes, with respect to classified information.

Senator SASSE. Is there any distinction between that statement and saying that no prosecutor would bring charges, which is, I think, what you said in your public statements the day that you made your announcement?

Mr. COMEY. Well, I think it is another way of looking at it. I think, given the evidence in this case, I still think that no reasonable prosecutor would try to bring this case.

Senator SASSE. OK. Thank you.

Secretary JOHNSON, last week, the Inspector General said that somewhere between 800 and 1,800 individuals were accidentally granted citizenship. Can you tell us the exact number?

Secretary JOHNSON. The exact number is 750. The Inspector General settled on this number of 858. As we looked closer, not all 858 were actually granted citizenship.

Senator SASSE. Can you distinguish some of those categories inside of the 750? And, were any of them from special interest countries?

Secretary JOHNSON. Not offhand. I cannot give you that breakdown offhand. I suspect it is a knowable fact, which we can provide you. I will say, Senator, that we have been reviewing all of these cases, as we have been going through the process of converting the physical fingerprints to digital, and there is a process under way, right now, and an investigation to denaturalize a number of those, who should not have been naturalized, as a result of what occurred. And, that is under way—and we are going to continue to do that.

Senator SASSE. Were any of them from Iran, Syria, or Libya?

Secretary JOHNSON. I would have to check. I do not know, sitting here right now, sir.

Senator SASSE. This is an honest question, not a “gotcha” question. How would you not know that? Why would that not be something that is urgent to you—to understand the categories under the 750—

Secretary JOHNSON. It is a knowable fact. I can get you the information. Just sitting here right now, I do not have the list in front of me. And, I do not want to be wrong.

Senator SASSE. Do you think any of them were terrorists?

Secretary JOHNSON. I have no basis to believe that any of them were terrorists or suspected terrorists.

Senator SASSE. Director Comey—

Secretary JOHNSON. We are going through the process now, of investigating the cases. This is a legacy matter that goes back to the 1990s. And, we have been denaturalizing people as we go through this process.

Senator SASSE. But, these were 750 people that were under deportation orders. So, it would seem that as to the offensive versus defensive form of the question earlier—is there any more important defense than knowing if any of those 750 people were terrorists or likely terrorists?

Secretary JOHNSON. I agree with you—

Senator SASSE. What is the priority that would take precedence over that?

Secretary JOHNSON. I agree with your question, sir, and that is why we are going through this process, right now, to investigate each one of these cases, using the resources we have.

Senator SASSE. But, in the 11 days—or whatever it has been—since the IG made your Department aware of the problem, you did not think to ask if any were from Libya or Syria?

Secretary JOHNSON. Senator, just sitting here, right now, I cannot give you the answer to that question. It is an important question. Just sitting here right now, I cannot give you the answer to the question. And, I do not want to be wrong.

Senator SASSE. Thank you.

Director Comey, I think the IG said that at least 2 of the then 858—I will take Secretary Johnson’s point, it may be 750. At least two of them had previously been referred to the FBI for possible terrorist linkages. Do you know anything about that?

Mr. COMEY. I do not.

Senator SASSE. So, when the IG reveals that to us—help us—help Nebraskans understand how the Executive Branch works together. The IG says these people have been referred to the FBI. Your Agencies are or are not talking to each other? How can we explain that to our citizens?

Mr. COMEY. Your question was to me, personally. I will find out, after this hearing. I am highly confident people in our Counterterrorism Division have been talking to DHS to find out what is there, and to look at it. It just has not been briefed to the Director, yet.

Senator SASSE. Thank you.

Secretary JOHNSON. Correct.

Senator SASSE. The distinction between historic fingerprint records—and I know I am at time, so this one may turn into one of yours, by mail, for later. But, historic fingerprints versus digitized fingerprints—how long has that process been going on? And, when will it be completed?

Secretary JOHNSON. I expect it to be completed in the next 9 months. It has been going on for quite some time—possibly years, sir.

Senator SASSE. Before we had digitized fingerprints, though, we still had a process to decide who to let into the country—and not. So, that is not a sufficient excuse for what went wrong here, right? What happened to grant these 750 people, who were supposed to be deported—how were they granted citizenship? What was the mistake?

Secretary JOHNSON. They were granted citizenship at a time when the conversion was not complete. Therefore, the persons examining the records did not have the old fingerprints from the paper record. And, that is what happened.

Senator SASSE. Thank you. Thank you to all three of you.

Chairman JOHNSON. Senator Ernst.

OPENING STATEMENT OF SENATOR ERNST

Senator ERNST. Thank you, Mr. Chairman. Gentlemen, thank you for being here, today.

Secretary Johnson, if I could start with you, please. On June 29, Senator Grassley, Senator Sasse, Senator Fisher, and I introduced a bill called “Sarah’s Law” to amend the mandatory detention provisions of the Immigration and Nationality Act (INA) to require the Federal Government to take custody of anyone in the country illegally, who is charged with a crime that results in death or serious bodily injury. “Sarah’s Law”—and we have talked a lot about this as of late—was named in honor of a young woman from Iowa, who was killed in a drunk-driving accident, in Omaha, Nebraska. And, behind the wheel of the other vehicle was Edwin Mejia, who was in the country illegally and was driving drunk at three times over the legal limit. When local law enforcement reached out to the U.S. Immigration and Customs Enforcement (ICE), to see if they wanted

to detain the driver, before he could post bond, ICE declined to do so. And, Mejia subsequently posted bond and remains at large.

In a letter I received back in May, ICE acknowledged that, simply put, Edwin Mejia should be in custody and that his detention should have qualified as an important Federal interest, pursuant to the detention policies outlined in a memo you circulated in November 2014.

Since then, we have been told, by ICE, that they have instructed their field offices to consider anyone in the country illegally, who kills an American, to be an “important Federal interest” and a priority for detention and deportation. And, first I have to say, for the record, that I cannot believe that this was not a top Obama Administration priority to begin with. And, regardless of what has been said in the field offices—we have not received any confirmation that it truly was said in the field offices. So, we do not know if this is actually the policy of ICE now—or not. There is no written confirmation.

So, can you confirm that ICE field offices have been instructed to detain illegal immigrants who are charged—not convicted, but charged—with a crime that results in the death of an American citizen?

Secretary JOHNSON. I believe I can. I am very familiar with the case of Sarah Root. I have exchanged correspondence with Senator Sasse on this tragic topic. We have reiterated to the field, at my direction, that there is this important Federal interest provision in our priorities memo, which I issued in November 2014. That has been sent to the field. And, just yesterday, I was looking at our numbers of those in detention, and it is reflected in the implementation of the policy. So, we are detaining more people, when somebody in the field judges it to be an important Federal interest to do so.

Senator ERNST. Do you know how many times that important Federal interest has been used to detain someone?

Secretary JOHNSON. Not offhand, but it is reflected in the statistics that we are seeing now.

Senator ERNST. OK. So, we are seeing an increase, perhaps, in the number of people being detained by ICE?

Secretary JOHNSON. Yes, ma’am.

Senator ERNST. OK. And, do you have any updates, from the Department, on Edwin Mejia’s—where he is located or where we are on finding him?

Secretary JOHNSON. I know, from my communications with Senator Sasse—as I told him, we, along with local law enforcement, are looking for him.

Senator ERNST. Do you believe him to be in the country or elsewhere?

Secretary JOHNSON. I could not say.

Senator ERNST. OK. And, for Director Rasmussen, we will move on to a different topic. In your testimony, you noted, “Having passed the 15-year mark since 9/11, the array of terrorist actors around the globe is broader, wider, and deeper than it has been at any time since that day.” An issue that I have been focused on is the rise of ISIS in Southeast Asia. Is NCTC concerned with this?

And, what do you believe to be the potential impact on U.S. national security?

Mr. RASMUSSEN. That is a terrific question, Senator. I just returned from four nations in Southeast Asia, just within the last 2 weeks, myself, because I was concerned about how, as the caliphate has looked to expand around the world, there are certainly vulnerable populations in Southeast Asia, in a number of countries where the ISIL ideology could find fertile ground.

As you well know, in the period after 9/11, Southeast Asia was a very active theater for al-Qaeda, and the al-Qaeda-affiliated organization Jemaah Islamiyah posed a major threat in Southeast Asia to U.S. interests and to the interests of our partners. So, we have known, looking back, that this was always a potential hot zone, where ISIL might find the possibility to take root.

My trip out there was designed to kind of engage with our intelligence partners to make sure that we were doing exactly what Director Comey was talking about—a much more aggressive exchange of intelligence information that we need to—to be able to get ahead of this. There are foreign fighters, from that region, who have made their way into Iraq and Syria. Those individuals seek to identify individuals to send back to—or to connect with—back in their home countries. And so, the same phenomenon that the Europeans are dealing with—that our other partners are dealing with—is being seen in Southeast Asia. So, we are applying many of the same tools to try to get ahead of it there.

Senator ERNST. And, for Secretary Johnson and Director Comey, with those terrorist elements existing in Southeast Asia, do we see any implications of those potential members from Southeast Asia of ISIS or other terrorist-affiliated groups—do we see them traveling into the United States?

Secretary JOHNSON. Senator, the way I would answer the question is this: We continually reevaluate and evaluate our targeting rules—the rules that we apply for how we assess someone entering the country—or who wants to enter the country. And, based on threat streams, we adjust those so that, when people seek to come here—or come here—and they show up at the port of entry (POE), they will either be sent to secondary, or they may be denied entry, altogether, at the outset.

Senator ERNST. OK. Very good.

Director Comey, do you have anything to add?

Mr. COMEY. No, just that that threat underscores the importance of connecting ourselves to those partners in Southeast Asia, so that we know who they are worried about, so we can put them in our databases and so we can stop them from getting in here.

Senator ERNST. Very good. Gentlemen, thank you very much.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Heitkamp.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you, Mr. Chairman.

First off, Director Comey, thank you so much for coming to North Dakota to address what I think is a critical problem in our State, across Indian country. And, that is the lack of criminal justice support for native populations. I think you saw there the dramatic in-

crease in the amount of drug crime, in particular, but also sexual assaults. Many of the communities that I visit with tell me that they feel under siege. When I challenge them to say, "What are you doing?", they tell us that the communities are terrified. And so, I know you and I may have a disagreement about the need for additional resources, but we certainly want to find out what it takes to staff up—to protect these communities, especially given the unique role the FBI plays in Indian country, in terms of your primary jurisdiction.

I want to just make a point. I am just going to make some quick points and just get things on the record—probably I will not have as many questions.

One of the trends that I have seen, Director, with very many of the very high profile incidences of terror and mass shootings is a background history in domestic violence. I think that taking a look at the National Instant Criminal Background Check System (NICS)—taking a look at how domestic violence plays into this and what we need to do to, maybe, pay more attention to those early warnings of someone with a violent background, it seems—I am not saying every person who commits an act of domestic violence could become a terrorist, but, I think, if we looked at those circumstances, we are seeing more and more of that. So, I would just maybe follow up with a question on NICS, domestic violence, and what we are doing to close those loopholes.

Secretary Johnson—the Northern border—you were not going to come here without getting a question on the Northern border. Obviously, I am very concerned about staffing. I appreciate your response to Senator Tester's question about the need to continue our collaboration with Canada. We are blessed, on the Northern border, with a law enforcement relationship that has been historically very collaborative. And, I think we can double our impact on the border if we continue to advance the work that this Administration has started with the Canadian Government.

I want to talk about drugs on the Southern border. I have spent a fair amount of time on the Southern border. I think most of the ranchers down there would tell you now that they are not as concerned about trafficking in persons coming across the border, but they believe a great deal of drugs are coming across the border. In fact, I recently received a picture of a cannon that shot marijuana across the border. And, I know you have seen those as well.

Going back to the questioning—or the discussion with—I guess not much discussion—the diatribe with Director Comey—one of the challenges that we have is that methamphetamines in my State have gone from \$600 an ounce to \$300 an ounce. I honestly believe that is supply driven, and that we are seeing more and more coming into the country. If we are going to have a logical discussion about issues regarding immigration, we need to take a new look at border security and make sure that we are doing everything that we can to respond to what people on the ground are actually seeing. I really appreciate all of the men and women—blue and green—who work for your Agency and who are doing a terrific job.

The final point is, the great work that you are doing, in terms of outreach to communities that could, potentially, become radicalized. I think that is work that almost every community in

our State could benefit from—Minneapolis is, obviously, an area where you have done a great deal of work on anti-radicalization. We have populations that move from Fargo, North Dakota and from Grand Forks, North Dakota to Minneapolis. How do we take that program more broadly? And, as you said—I think, very correctly—you are not as concerned about radicalization—the message coming from the government may not be the most helpful message. How do we get this message into the community? And, how do we build those relationships long term?

Secretary JOHNSON. Well, first, if I, personally, do not make it to Fargo, others will, from my Department, for—

Senator HEITKAMP. Well, you are welcome in Fargo. You can visit the chipper. [Laughter.]

It is at the Visitor Center.

Secretary JOHNSON. Thank you. Senator. Listening to your questioning, I think the immediate answer I have is, it would be most important if community leaders could be encouraged to apply for some of our grants, in the future, for locally-based countering violent extremism initiatives. It seems to me that a community, like Fargo, could probably benefit from something like that.

Senator HEITKAMP. I am absolutely convinced that this community policing model that came out of the 1990s, where we actually have dialogues with community members, eyes and ears on the ground, and build the trust, is how we are going to do a much better job defending the homeland. But, also, the best defense is a good offense. I think that this is a great proactive measure that needs to be taken. And, please, I hope that, in the exit of this Administration, this is a project that continues to receive very high priority at the Department of Homeland Security.

So, thank you so much, Mr. Chairman. And, I will yield back the rest of my time.

Chairman JOHNSON. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman.

Gentlemen, thank you. Thank you for being here, and thank you for all you do for the country. You all stay at it all day, every day, and there is a lot that goes on, which most people do not know that you all do. So, we appreciate the work. You also can appreciate our second-guessing and looking over your shoulder all of the time, as we all have accountability. But, I want you to know we very much appreciate your work.

Secretary Johnson, could you also pass on my appreciation to Administrator Neffenger as well? He has had a very tough job and has made some serious transitions within the TSA, both in personnel and in process. I know a lot of that is still in process, but can you pass, on from our Committee and from me, that appreciation for the hard work that he has taken on there as well?

I know with my State as well—just on a purely parochial level, we have had conversations before about REAL ID and some uniqueness in Oklahoma, because we have a private system for issuing driver's licenses. So, it has been an ongoing process to be able to help try to figure out a way to be able to fulfill that, because of our unique system. Oklahoma is a little bit different from

some States, in that people, typically, do not mind going to get a driver's license, because it is a private entity that does it. And, it usually takes about 5 minutes. That is not true in a lot of other States, and we are trying to not lose that part, while we are still working through the REAL ID process. So, I appreciate the flexibility that has been there.

I want to talk briefly on several issues here as well. One is the growth of homegrown violent extremism. This is one of those threats that is incredibly difficult to be able to track, but it is trending the wrong direction. And, trying to figure out both the inspiration side and tracking how people are inspiring those, in the United States, and how we move, as, Mr. Comey, you have mentioned often, the "flash-to-bang" ratio—that time period getting very close together. So, what do you see currently, nationally, on homegrown violent extremism, and the trends?

Mr. COMEY. We continue to work cases, trying to assess where someone is on the consuming to acting spectrum, which, as you said, is often very short and unpredictable.

Senator LANKFORD. Right, and it is not illegal to be able to look at Anwar al-Awlaki's sermons, for instance. But, suddenly, those that are looking at it then turn violent, fairly quickly—but not all of the people do.

Mr. COMEY. Right. It is even protected speech to say, "I am a fan of the Islamic State," so-called. And so, our challenge is to figure out where people are with that. We still have about 1,000 open investigations on that. If there is any good news—and I do not want to squeeze it too hard for good news—it is that the rate of increase has slowed a little in recent months.

Now, my hope is that it is going to follow the same trajectory as the traveler numbers, and head downward. But, it has not headed downward, yet. We are still opening and closing, and it is ticking up slightly.

Senator LANKFORD. So, we have thousands of foreign fighters, who have traveled to Syria and Iraq to fight with the Islamic State, that have returned back to Europe. We have a limited number—what is our number that we think have tried to travel to fight with the Islamic State—or at least traveled to that region, from the United States?

Mr. COMEY. With us—with the Islamic State—it is a number in the dozens.

Senator LANKFORD. OK. So, we are in the thousands, though, of people that have traveled to that region and who have returned to Europe. How are we doing now, with tracking those individuals that have been traveling from Europe to the United States?

Secretary JOHNSON. Senator, first of all, we have added a lot of security around the Visa Waiver Program. We get more information through the Electronic System for Travel Authorization (ESTA), which has actually been a productive exercise. We have denied ESTA travel—visa-free travel to a lot of people, as a result of the added security.

Senator LANKFORD. Help me understand the phrase "a lot of people." Give me an example of what that might be.

Secretary JOHNSON. I have seen the statistics. In the first year that we added questions to the Electronic System for Travel Au-

thorization, I think, we denied—as a result of those additional questions—people, I believe, in the thousands. I can get you the exact number. It is an available number.

Senator LANKFORD. OK. That would be helpful.

Secretary JOHNSON. The Congress, last year, passed additional security, which has also limited the ability to travel here visa-free. Congress gave me the authority to add countries to the list for which, if you visited them, you cannot come here visa-free. And, I took advantage of that. So, we have added security there.

More broadly, however, I think it is incumbent on us to continue to work with the EU—with European nations on the sharing of Advance Passenger Information (API) and Passenger Name Records (PNR) data, more Federal air marshal agreements, and more preclearance—forward deployed. We used the football analogy, earlier, where we are defending on the 1-yard line. I want to defend on the 50-yard line. So, preclearance is an opportunity to screen people on the front end of their travel to the United States. We have had a number of foreign airports that have indicated an interest in building that with us. And, it is a priority of mine, and we are going to keep at it.

Senator LANKFORD. OK. Let me bring in several topics here, as we try to blitz through this. Secretary Johnson, this is an internal issue, but it is one of the things that I am also concerned about and that we have clear oversight on. And, one is dealing with human resources (HR). When DHS was formed, you had all of these different HR systems. As I recall, the number, in 2011, was still reaching about 442—or somewhere through there—total different, independent systems—still within DHS, dealing with HR. 2011 came, and DHS set its standards. So, there are 15 main areas and 77 projects that we want to be able to accomplish. The Government Accountability Office (GAO) came out and said, at the end of 2015, that, of those 15 projects named in 2011, only one of them has been accomplished—of the areas—and of the 77 projects within that, I believe it is two or three that have been completed. And so, what I am trying to figure out is, give me—that was at the end of 2015. At the end of 2016, where do you think we are going to be, in trying to compile all of these different HR systems, so we can have a more efficient inner structure?

Secretary JOHNSON. It is a good question. As part of my “Unity-of-Effort” initiative, we have been looking to streamline the HR process and reduce the number of these systems. I would have to get you the exact number. I do know that GAO has been very complimentary of us for addressing all of the high-risk items on their “High-Risk List,” and we hope to get off of that list at some point in the not too distant future. But, I can get you the precise numbers.

Senator LANKFORD. OK. That would be helpful to know. Just trying to be able to track the process, internally, there.

Of the 148,000 older fingerprint cards that Senator Sasse mentioned before, where are we, as far as getting those digitized?

Secretary JOHNSON. Nine months.

Senator LANKFORD. Nine months—to be complete, from now, of all 148,000?

Secretary JOHNSON. Nine months from now to be complete.

Senator LANKFORD. OK. Mr. Comey, let me ask you about drug enforcement. And, this is one of the areas I am concerned about with the FBI. You have so much on your plate, but, obviously, dealing with drug enforcement, specifically, dealing with Central America—you have a very unique connection, where there is both gang involvement and what is destabilizing Central America—much of it is coming from the United States and the movement of drugs. Again, it is destabilizing, so it is causing immigration issues and a lot of crime and grief on our streets, for families. Give me an update on where you see the trends right now, in the movement of drugs in the United States, and the gang activity in the United States.

Chairman JOHNSON. I will let him get away with it, because we are down to a couple of Members, but answer briefly.

Mr. COMEY. The two major trends to highlight—nearly all of the heroin coming into the United States and nearly all of the methamphetamine is being produced in Mexico, now—and a wave of highly pure heroin has been washing from the east coast toward the west, and a wave of highly pure methamphetamine has been washing from west to east. Those waves are now overlapping. Those are Mexican trafficking organizations that are using gangs in the United States as their distributors, but the importers are the Mexican trafficking organizations. Those are the two most important macro trends, at this point.

Chairman JOHNSON. Thank you, Senator Lankford.

This is a pretty interesting Committee. I do not think people realize that we really have two Committees in one. We have the homeland security side, and then we have the governmental affairs side, which is really the Senate's oversight Committee. We have, as a result, oversight pretty much over the entire Federal Government. We also have legislative jurisdiction, which we have tried to use, with Secretary Johnson, in trying to codify some of the good work he is doing to improve the Department of Homeland Security.

But, we also have legislative jurisdiction over national security procedures and Federal records. And, I would be remiss, in my duty as Chairman of the Committee, if I did not delve a little bit, in terms of the mishandling of classified information by the former Secretary of State.

Classified information and the protection of it is extremely important. If you mishandle classified material, you can put people's lives at risk. Certainly, if our adversaries have access to it, it can change their calculation. Their behavior may change. I cannot think—and, having been in business, the best possible thing I could get would be the email communication of my negotiating partners, to figure out where they are coming from. And, let us face it, if adversaries have emails, they could, potentially, blackmail government officials. So, the handling of classified information is an incredibly important issue. It is something incredibly important to protect.

Director Comey, when all is said and done, there were seven emails that are so top secret that not one member, I believe, on this Committee—maybe somebody on the Senate Select Committee on Intelligence (SSCI)—can have access and actually look at those

things. In your investigation, were you able to look at those—or was any member of the FBI?

Mr. COMEY. Yes, Senator, because I have the appropriate clearances, that was a particular special access program to be able to view that material—as did all of the investigators and analysts working on the case.

Chairman JOHNSON. OK. But, it does say something when Members of this Committee do not have access to that, correct? These emails, in your investigation, were, obviously, outside of a classified system, correct?

Mr. COMEY. They were on an unclassified system, in fact.

Chairman JOHNSON. So, they were clearly outside of a classified system. And, anybody emailing the Secretary understood that, correct? I mean, it is pretty obvious, when you are sending an email, whether it is to `statedepartment.gov.class` or to `Clinton.inc`—or whatever the email handle was. Correct?

Mr. COMEY. I am not sure that individual emailers understood what the Secretary's email address was, because it was not visible in a lot of people's fields. It would just have an initial—

Chairman JOHNSON. How many—

Mr. COMEY. But, they knew—everybody emailing knew they were not on a classified system.

Chairman JOHNSON. And, that is the only system that should be used for classified material, right? It is not like you have three, four, or five different email systems you should be communicating our Nation's top secrets on, correct?

Mr. COMEY. Correct. The FBI has three systems: unclassified, secret, and top secret. And so, you are supposed to use, for obvious reasons, the system appropriate to the information.

Chairman JOHNSON. So, if you are not using that classified system, you are mishandling classified material?

Mr. COMEY. Yes.

Chairman JOHNSON. In your press conference, you said that no reasonable prosecutor would bring this case. But, in fact, there are a couple of cases I just want to see if you are aware of: the case of Naval Reservist Bryan Nishimura, in Afghanistan, in 2007 and 2008. Now, he was not prosecuted, because, in order to avoid prosecution, he pled guilty to the unauthorized removal and retention of classified materials. A judge fined him \$7,500, and he was ordered to surrender his security clearance.

Another case was of James Hitselberger. He was a contractor translator at the naval base in Bahrain. He pled guilty to a misdemeanor for his handling of documents in 2014. He was sentenced to time served after 2 months in a D.C. jail and 8 months of home confinement.

How are those cases different than what happened with the former Secretary of State?

Mr. COMEY. All of the cases that were prosecuted, including—I definitely know the Nishimura case, for sure. I went through 40 years of cases. So, in June and July, I had them all in my head. I do not remember exactly the second one. But, I am highly confident that all of the cases that were prosecuted, including the misdemeanors, involved obstruction of justice and vast amounts of material handled in such a way that it was clear they were inten-

tionally mishandled. Nishimura is a great example—a huge amount of stuff that he tried to destroy, once the investigation began. So, there were aggravating factors that led the Department of Justice to bring those cases.

Chairman JOHNSON. Did you look at any aspects of obstruction of justice in your investigation, with any of the players, in this episode?

Mr. COMEY. Sure, yes.

Chairman JOHNSON. And, you found none? I mean, on March 2, the “New York Times” reported, for the first time, that Secretary Clinton had a personal email account. On March 3, Chairman Trey Gowdy sent a letter to Secretary Clinton’s attorney, requesting they preserve the records. The following day, Chairman Gowdy issued a subpoena. And, somewhere between March 2 and March 31, Platte River Networks’ employees, basically, destroyed evidence. Is that not obstruction of justice?

Mr. COMEY. We looked at it very hard, to see if there was criminal obstruction of justice. In fact, one of the people the Department granted immunity to was the fellow involved in deleting that stuff, after the public notification and the hold letters. And so, we looked at it very hard. We could not make an obstruction case against any of the subjects we looked at. The Department granted immunity to the one fellow, who had erased the stuff, so that we could figure out, “Did anybody tell you to do this? Did anybody ask you to do this?” to see if we could make an obstruction case. We could not.

Chairman JOHNSON. My concern, when all is said and done, with what Secretary Clinton did, is that, by not prosecuting anybody in this case, we really do signal that we have a two-tiered justice system here. And, what is that going to do, in terms of other people that are charged with the responsibility of properly handling classified information? Are you also concerned about that, in terms of what actions you have taken?

Mr. COMEY. I very much disagree with your characterization. I think, had we recommended prosecution, it would have been a two-tiered justice system, because we would have been recommending it in a circumstance where, for the ordinary Joe and Jane, we would never have considered it. My goal in this case was to treat people—as it has been in my entire career—fairly, without regard to their rank in life. This case was done in that way, and the decision was made in that way. So, I think to do otherwise would have been “two-tiered.” I am very proud of the work we did. I know it generated a lot of controversy, but I am very proud of the work we did.

Chairman JOHNSON. I have just a couple of seconds, so I will not go down my next line of questioning. I might go to a second round or a third round. Senator Carper.

Senator CARPER. Thank you, Mr. Chairman.

Is there anything else you would like to say, with respect to the last question or the last line of questioning from the Chairman, Mr. Comey?

Mr. COMEY. No, I do not think so, Senator.

Senator CARPER. OK. Mr. Chairman, I would like to ask that something be submitted for the record.¹ It is actually a series of email exchanges between Secretary Clinton and former Secretary of State Colin Powell, who is one of the people I most admire.

Chairman JOHNSON. Without objection.

Senator CARPER. I am going to pivot here and change the subject a little bit. And, this would be one for Secretary Johnson. I would like to talk about the National Protection and Programs Directorate (NPPD). As the Secretary knows, I am not a big fan of a lot of acronyms, and it always was not clear to me why we would sort of—instead of actually calling an Agency what it—by a name that would actually tell you what it does, we call this one NPPD. And, I understand and very much support your efforts—the Department’s efforts to streamline that particular entity and actually to call it by something that explains or conveys what they actually are responsible for doing. And, instead of calling it “NPPD,” to call it the “Cyber and Infrastructure Protection Agency,” which makes a lot of sense. As my father would say, “Well, that is common sense, Tom.”

So, talk to us about why the streamlining and the name change are appropriate, please.

Secretary JOHNSON. First, it is so that the name is simpler. Right? I always have to think about what NPPD stands for.

Senator CARPER. Me, too.

Secretary JOHNSON. And, it is a very generic name. We need an Agency of our government devoted to cybersecurity. And, the substance behind our proposal to restructure this thing is so that NPPD sheds some of its less critical and more administrative missions and focuses on just two things—cybersecurity and infrastructure protection—and focuses on both in a way so that the two missions are merged. We ought to have a focus on the cybersecurity of critical infrastructure and the cybersecurity of infrastructure. And so, we want to take those two missions, put them together, and have a lot of the same people focused on both of those missions in a more effective and efficient Agency, called the “Cyber and Infrastructure Protection Agency.” We need an Agency of our government devoted to those two very important things.

Senator CARPER. Good. I approve that message.

Secretary JOHNSON. And, it will require an act of Congress to make all of that happen, which is why we are seeking the help of this Committee.

Senator CARPER. Good. Let us talk a little bit about EINSTEIN. I understand the Department has made a lot of progress on the implementation of the new cybersecurity information-sharing portal and on EINSTEIN. And, these are, as you know, really important programs that can, we think, help us on the cybersecurity front across our Federal Government—as well as in the private sector. And, I would like for you to drill down just a little bit more on these two programs, if you would, as well as the status of EINSTEIN implementation across Federal civilian Agencies. And, are there any Agencies you are concerned about not meeting the statutory deadline? I think it is December of this year. What is the sta-

¹Information submitted by Senator Carper appears in the Appendix on page 85.

tus of the cyber information-sharing portal that we established, in law, at the Department of Homeland Security? Are companies starting to share their information?

Secretary JOHNSON. We are, as you know, Senator, deploying EINSTEIN 3A, right now, which has the ability to block unwanted intrusions in the Federal civilian .gov system. About a year and a half ago, we had only covered about 20 percent of the Federal civilian workforce. Today, as we sit here, we are up to about 65 percent, and we have memorandums of understanding (MOUs) with all but three Cabinet-level departments. I scheduled a meeting with the Secretary of one of those Cabinet-level departments, and lo and behold, the MOU fell into place before we had the meeting.

Senator CARPER. Maybe you have to schedule a couple more meetings.

Secretary JOHNSON. And, the other two, I am confident we are going to have very soon as well—and those will be the last three large remaining ones. I am not referring to anybody at this table here. And, I believe we are going to meet the statutory deadline.

Senator CARPER. That would be great.

Secretary JOHNSON. I think it is critical that we do that.

Senator CARPER. Please share a little bit of the status, if you will, of the cyber information-sharing portal that is being established at DHS, please?

Secretary JOHNSON. We now have automated information sharing at the National Crime Information Center (NCIC). We put it in place in March 2016. And so, it is now a matter of getting Agencies and companies online with this new capability. We have the intelligence community (IC), and we have the law enforcement community—the Federal Government—online with this—a few other Departments—and we have a number of large companies in the private sector and in information-sharing organizations. But, there is a lot more to do there.

And so, I am continually promoting this new capability, in the private sector, in particular—and so that is a work in progress.

Senator CARPER. Alright. Good. I think I mentioned to you, I went down to the Federal Law Enforcement Training Center (FLETC), in what used to be Naval Air Station (NAS) Glynn, Georgia. And, I was really impressed by what I saw. I spent a great day there—a wonderful day there, with a lot of very dedicated people, doing good work for our country. And, I want to talk just a little bit—some of them were TSA. They are now running a TSA training academy there to try to eventually train everybody who works at TSA. And, I have been especially impressed with the steps that Admiral Neffenger has taken at TSA. I remember the day you called me to say, “We have somebody we want you to consider for confirmation as head of TSA, this guy named Neffenger”—I think a three-star admiral. You said, “He is a good one.” And, boy, you were right. You were right.

Just do us a little bit of a favor and update us on how TSA has been doing after some very tough sledding earlier this year. How are they doing?

Secretary JOHNSON. Well, first, the day Pete was sworn in, I handed him a 10-point plan for improving aviation security, in reaction to the Inspector General’s covert testing last year. TSA has

done an excellent job at implementing that 10-point plan, including investments in new technology and less managed inclusion at airports—the longer line, where you take people from the longer line and put them in the shorter line. That contributed to the additional wait times that we saw this spring, along with the increased travel volume. We addressed that by, with the permission of Congress, expediting the hiring of new Transportation Security Officers (TSOs) and converting a lot of them from part-time to full-time. We have addressed the wait times. We are continuing to invest in new technology, and I think we have to build back that workforce. And so, we have a long-term plan, with Congress, to do that.

Senator CARPER. Mr. Chairman, just maybe another minute—and this is the last time we will, probably, have Jeh before us. As much as I admire, respect, and feel gratitude toward Mr. Comey and Nick, I just want to say what a joy it has been to work with you. Thank you for your leadership. Our job was to try to make sure you were surrounded by a first-rate team, and the folks that you and the President gave to us to consider really are a first-rate team. We are really pleased with that.

Ever since this Department was created, they have suffered from bad morale. With all of these disparate Agencies all over the place, it made it hard to communicate and to work together. For a long time, we did not have confirmed leadership at the top, and we have tried to address all of that and provide reasonable amounts of support financially. And, the morale of the Agency has finally turned around for the better. Would you just take a minute and talk about that—just a minute—and tell us what advice you would give to your successor on the importance of continuing some of the management reforms at the Department.

Secretary JOHNSON. I would say that it is important to continue what we have begun. Particularly, when it comes to employee satisfaction, we turned the corner—and I hope that continues.

The Deputy Secretary and I did, this year, 55 employee engagements in 22 different cities, to hear concerns and to meet employees. We have a more transparent hiring system and a more transparent promotion system. We have, as you know, a Department-wide mission statement. And, we have been stressing, to our workforce, the importance of their mission. And, I think people are responding.

I think it is significant to note that the levels of employee satisfaction went up the most significantly in the immigration components. ICE went up seven full percentage points. U.S. Customs and Border Protection went up four percentage points. And, these are two very large government Agencies, in and of themselves. I am very proud of their progress, and I think we need to continue that—along with making our Department more centralized, less stovepiped, and more streamlined.

So, I hope that happens. And, I will note that it was Members of this Committee, including you, in particular, Tom, that told me that management reform needed to be one of my priorities, if I was confirmed. And, it has been.

Senator CARPER. Thank you.

Chairman JOHNSON. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Thank you, Mr. Chairman. And, thank you to our witnesses here, today. I thank you for your service, every day, in defense of our Nation. You have a very tough task, and you perform it with professionalism and passion. Thank you for that.

I also wanted to say thank you to Secretary Johnson. I know this may be your last appearance. You have heard many of my colleagues praise your efforts. I want to join in that chorus. I appreciate your efforts, particularly, in Michigan—especially the many trips that you have made to our State, particularly, to engage the community. As I am sure most folks are aware, we have a very large Middle Eastern population in Michigan—one of the largest concentrations anywhere. You have been actively engaged in that community, and I know that has been a part of your efforts to make sure that there is a community approach to dealing with the threats that are there.

You were recently there in August. We spoke briefly before the beginning of the hearing. You were meeting with some police officers of Middle Eastern descent. If you would, just briefly—I think folks need to know what is happening in a vibrant Middle Eastern community, in Michigan, and how that can be a template for how we handle this issue around the country.

Secretary JOHNSON. Senator, you have, in Michigan, some really dedicated, terrific DHS personnel, who took the initiative to form this Middle Eastern Law Enforcement Officers Association (MELOA), which consists of largely—but not exclusively—DHS people: CBP, ICE, and TSA—centered around the Detroit-Dearborn area.

I went out there for a visit, to meet with them, several months ago. I think it was January. I was really impressed, and I encouraged them to grow nationally for a couple of reasons: one, community outreach; two, recruiting; and, three, cultural sensitivity, when it comes to others in law enforcement.

And, when I went back in August, I was pleased to see that they were having a national-level meeting. Their organization has grown. And, I would like to see this concept grow across the entire Federal Government. And so, I have encouraged them to do that. And, Senator, I encourage you to get to know these people and support them as well. They are a terrific group, centered right there in your State.

Senator PETERS. Well, I look forward to it. And, I appreciate your efforts in shepherding that forward and in giving them the support that they need to continue to grow. And, hopefully, we will be able to involve all sorts of agencies, both local and Federal, in that kind of community.

I also want to change course a little bit and just talk about some potential future threats. Certainly, we have had a discussion today about a variety of immediate threats that we have to be very concerned about—and you are actively engaged. But, also, I stay up at night thinking about some of the future threats that may be there and whether we are adequately prepared.

One area that I have thought about—and we had some testimony here, before our Committee, not long ago—dealt with biodefense and bioterrorism, and the potential for that. We heard from former

Homeland Security Secretary Tom Ridge and Senator Joe Lieberman, regarding some findings from the Blue Ribbon Study Panel on Biodefense—and, basically, they declared that the United States is unprepared for biological threats.

The Government Accountability Office also has found that the biodefense enterprise is fragmented and is lacking the strategic oversight necessary for efficiency and accountability. And, certainly, I am concerned that a bioterror attack could be the next threat that we have to deal with—and we need to be prepared.

Secretary Johnson, I am particularly interested in DHS's use of the BioWatch program, which was developed to provide early detection of a bioterrorism event. As you know, last year GAO identified flaws with BioWatch, including that it is not really possible to test it in an operational environment. So, could you give us an update on BioWatch and some of your efforts related to bioterrorism, please?

Secretary JOHNSON. Senator, it has been a focus of mine. We have an office and a mission dedicated to the chem-bio threat to the homeland. I would be happy to give you a fuller written report on exactly where we are with BioWatch. But, this has been a focus of mine. And, obviously, it has been a focus of others, including Secretary Ridge.

The way I look at it is this: There are threats—and all three of us deal with this every day. There are threats that are high probability, and then there are threats that are perhaps less—lower probability, but high impact and high cost. And, we have to be responsible and keep our eyes on all of it. And, that includes the chem-bio threat to the homeland. But, I can get you a fuller report, in response to your question, sir.

Senator PETERS. Well, I would appreciate that.

I realize that you have multiple threats, and you do have to make those kinds of assessments on a regular basis. But, certainly, something of this nature, as you mentioned—even if the probability is maybe lower at this time, the impact is significant. And, when you look at some of the new technologies that are coming on board in the biotechnology sphere—Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) technology, for example, which could be used in some very nefarious ways—it certainly has incredible potential. But, also you can buy these kits fairly inexpensively, and this could present some significant issues.

In my remaining time, I just want to touch on cybersecurity—another area that is critical for us and perhaps one of the biggest threats that we have as a country. I had the opportunity to be out yesterday and visit with folks at the National Security Agency (NSA) and with the Cyber Command. And, I am encouraged by the cooperation that I saw. I know a couple of you have mentioned how we are now working together on cyber—all of the Agencies coming together. I saw that, firsthand. It was refreshing to see.

But, I would just like a brief comment on an area that I see as a vulnerability that we have to be thinking about—that, when it comes to cyber risk, it is usually the weakest link where the bad guys are going to go. And, although the Agencies have hardened systems and our Departments have done it, I think of small local governments and I think of small businesses—and others. We

know some of the attacks that we have seen—cyber attacks—have gone through contractors that are small contractors tied to a larger organization. So, I see some significant threats, potentially, through local governments, municipalities, as well as small businesses.

Are there things that we should be doing, here in Congress, to aid those efforts? Because, I know all three of you are very aware of that.

Secretary JOHNSON. I will just start really quickly. First of all, I am very appreciative of the law Congress passed last year on cybersecurity, which has greatly aided what we do in DHS. When you talk about the weakest link—the weakest link is always the employee vulnerable to an act of spear phishing. And so, the very basic thing that all of us need to do is raise employee awareness among our respective workforces to the hazards of spear phishing. The most sophisticated attacks very often occur just simply through an act of spear phishing.

Chairman JOHNSON. Senator Booker.

Senator BOOKER. Director Comey, I would like to change the direction of my questioning, specifically, to issues of race in America. There has been a lot of talk recently about law and order. And, you and I both—you, in your position, and me, when I was mayor and had a city with high levels of violence and crime—really did focus on law and order. And, it is critically important. But, we make a distinction in America, between law and order, which is a baseline—but we seek a higher level of standard—and that is justice. We pledge allegiance to this idea of liberty and justice for all. Our highest ideal is on the Supreme Court building: “Equal justice under the law.”

Now, in Birmingham, in 1960, there was law and order, but there was a clear lack of justice. And, many people complained when some rabble rousers—outside agitators, came in, literally, breaking some laws, actually, but exposing the fact that there was law and order, but without justice.

Now, Martin Luther King wrote eloquently in the letters from the Birmingham jail about that distinction—really focusing on the difference between law and order—which he used Germany, and other areas, as examples of places that had law and order, but did not have justice. We are Americans, and we strive for that ideal.

Now, what frustrates me is, 50 years from that time, we still seem to be dealing with a lot of the same issues. The National Advisory Commission on Civil Disorders, also called the Kerner Commission, which was put forth by President Lyndon Johnson 50 years ago, was seeking to diagnose why there was so much violence and rioting in cities—as well as nonviolent protests—going on. And, the report identified police incidents as the most common cause of riots and criticized the overpolicing of black neighborhoods.

Now, what frustrates me is that you read the Kerner Report, you read the letters from the Birmingham jail, and you read your words, sir—your courageous words—and, you see, we are still struggling from those issues.

Now, you gave a speech that I found amazing. I actually, used your speech in my book that I wrote. The “New York Times” called it “an unusually candid speech,” and, for the record, this is what

you wrote: “With the death of Michael Brown in Ferguson, the death of Eric Garner in Staten Island, the ongoing protests throughout the country, and the assassinations of New York City police officers, we are at a crossroads.” You stated, “As a society, we can choose to live our everyday lives, raising our families and going to work, hoping that someone, somewhere, will do something to ease the tension—to smooth over the conflict. We can roll up our car windows, turn up the radio and drive around these problems, or we can choose to have an open and honest discussion about what our relationship is today—what it should be, what it could be, and what it needs to be—if we took more time to better understand one another.”

Those are your words, sir.

“Much research points to the widespread existence of unconscious racial bias. Many people in our white majority culture have unconscious racial biases and react differently to a white face than to a black face. In fact, we all, white and black, carry these biases around with us.”

“But if we cannot help our latent biases, we can help our behavior in response to these instinctive reactions, which is why we need to work to design systems and processes that overcome the very human part of us all. Although the research may be unsettling, it is what we do next that matters most.”

You were incredibly courageous in this speech talking about racial bias in policing. You and I both have an adherence to the idea of data. We have wild conversations in America, and sometimes I listen to them—and it seems like we are not even talking to each other—we are not leading with courageous empathy.

But, what I am frustrated about is, while I think we need that empathetic—courageous empathy to begin to create the understanding to heal, as a country, we still, consistently—50 years since the Kerner Report—based on data—have different standards of justice being applied to different communities, in our country, which is creating understandable tension. And, frankly, if we saw the overpolicing that the Kerner Report talked about being done in other areas—of affluence—we would have a very different reality in American politics, because it would not be tolerated.

Now, you go on in this great speech to talk about specific needs that we have, if we are going to correct this problem. You state: “Not long after riots broke out in Ferguson late last summer, I asked my staff to tell me how many people shot by police were African-American in this country. I wanted to see trends.” You wanted the data.

I continue, in your words: “I wanted to see the information. They could not give it to me, and it was not their fault. Demographic data, regarding officer-involved shootings, is not consistently reported to us through our Uniform Crime Reporting (UCR) Program. Because reporting is voluntary, our data is incomplete and, therefore, in the aggregate, is not available.”

“I recently listened to a thoughtful big city Police Chief”—I stop here, and say that you and I both know there are lots of police departments that are trying to do very good things about confronting implicit racial bias. There are a lot of good, thoughtful leaders in this country, who recognize, like you do, that this is a problem.

I continue, in your words: “. . . thoughtful big city Police Chief express his frustration with that lack of reliable data. He said people did not know whether the Ferguson police shot one person a week, one a year, or one a century, and that in the absence of good data, all we get are ideological thunderbolts, when what we need are ideological agnostics, who use information to try to solve a problem.” And, you say, “He is right.”

And so, I do not want to be here 50 years from now—or listening to my kids and grandkids struggle with what should have been done in the 1960s, when thoughtful police leadership, like you, called for understanding this data of what does exist in our country, which is racial bias. And so, I have put forth legislation, saying, “Hey, let us get away from the ideological thunderbolts and get the data.” We cannot solve a problem unless we measure it. You are a manager of an Agency. I was a manager of a city. If you cannot measure it, you cannot manage it.

And so, I want your opinion on, basically, what you stated clearly—on the need for a national collection of data on implicit racial bias and on police interactions with communities.

Chairman JOHNSON. You can provide that as a written answer to that question.

Senator BOOKER. Sir, that is—you allowed so many other people to go over. My time has just ended. Why—

Chairman JOHNSON. Not really. I am going to ask for another round, and you can have another round. OK. I am going to keep this to 7 minutes.

There are three questions I want to ask, based on your testimony, as well as other questions asked during the hearing.

First, Secretary Johnson, it appears now that this Administration has let in about 10,000 refugees from Syria. I have, certainly, been on the record saying that one of the ways we could minimize any kind of risk would be to establish criteria. I have suggested for it to cover women, children, and the relatives of Syrian-American citizens that have the financial wherewithal to support them.

Is the Department, in any way, shape, or form, establishing criteria—or are we just vetting whoever the agency from the U.N. is providing us, in terms of asking us to take in refugees?

Secretary JOHNSON. We established criteria in the following sense: Between us, the Department of State, and the United Nations High Commissioner for Refugees (UNHCR), we focus on people who we think would be good candidates for resettlement in the United States. That is number one.

We have criteria, in the sense that we have added security checks to the process. And, if you meet certain criteria, there is going to be extra vetting. That was particularly true around Syrians. And so, we made the 10,000, frankly, by surging a lot of resources and adding a lot of people to it. But, we do have criteria. The criteria are not all public, and they should not be. But, we added security to the process—to the vetting process.

Chairman JOHNSON. So, you are fairly confident that the vetting has been robust—we have not taken any risks? I am the lead sponsor of the American Security Against Foreign Enemies Act of 2015 (SAFE Act) that would have asked you three gentlemen to certify

that. But, are you very satisfied that the 10,000 Syrians we have let into this country represent no risk to America?

Secretary JOHNSON. I am satisfied and comfortable that we put a lot into this process, with a lot of additional security and a lot of additional person power. And, I know for a fact that an awful lot of the 10,000 are families, women, and children, who are fleeing violence and fleeing terrorism—and who will be honest, hard-working people in this country.

Chairman JOHNSON. OK. In testimony, we talked about more robust uses of social media.

Secretary JOHNSON. Yes.

Chairman JOHNSON. Looking at that, when we are evaluating and vetting refugees—can you describe that in a little greater detail? One of the things I have suggested—I have certainly asked people—why do we not have it so anybody seeking refugee status comes in, with their devices—and, basically, have a plug-in program that can very rapidly scan these things. How are you doing it? And, are we trying to utilize technology to the maximum effect to do what I am suggesting?

Secretary JOHNSON. Senator, I want to expand the use of social media, not just for refugee vetting, but for visa-free travel, for example. We have a notice and comment period we just completed on adding social media questions in the ESTA system, right now.

Chairman JOHNSON. But, again, those are questions. Is there any automated system where, literally, you ask people to come in with their devices, whether they are seeking a visa or whatever—

Secretary JOHNSON. We have a system—

Chairman JOHNSON [continuing]. You just plug it in and, bam.

Secretary JOHNSON. The answer to your question is, we have a system for vetting social media. We need better technology, so that it is not manual.

Chairman JOHNSON. So, right now, it is manual?

Secretary JOHNSON. It is manual and it is time-consuming, which is why we need investment in the technology, so that we can look at social media, not just for refugee vetting, but for a whole host of things that this Department—and I suspect other Departments—use it for.

Chairman JOHNSON. My guess is that that is technology that ought to be rapidly developed. Am I incorrect there? Either Director Comey or Director Rasmussen, can you weigh in on that, one way or the other?

Mr. RASMUSSEN. I do not have any specialized knowledge on that particular question.

Mr. COMEY. I do know it is something that we work hard to develop the technology for—for our investigations—to go through huge amounts of seized media and publicly available social media. So, there are tools out there. Whether it is fit for this purpose or not, I do not know.

Chairman JOHNSON. I would suggest your Department and your Agency work together on that.

Finally, Director Comey, I do want to talk a little bit about these terror “watchlists”, because I think we are throwing a lot of terms around, and people do not really understand them. So, I just want to make sure people understand what we are talking about here.

From my understanding, the overall massive database is really the Terrorist Identities Datamart Environment (TIDE). Again, I am not sure what is law enforcement sensitive, so I do not want to talk about numbers—foreigners compared to Americans. A subsidiary list of that is called the Terrorist Screening Database (TSDB). And then, much smaller subsets of that are the No-Fly List and the Selectee list, correct?

Mr. COMEY. That is correct.

Chairman JOHNSON. None of these lists were ever developed—they were developed for law enforcement use, to give you an indication of whether or not you should investigate somebody—or somebody should be pinged for further investigation, correct?

Mr. COMEY. They are intelligence and law enforcement databases. There are standards to get identities in there, but their primary purpose is currently for that.

Chairman JOHNSON. They are far from perfect, correct?

Mr. COMEY. Correct.

Chairman JOHNSON. The standards for getting on to those databases are not exactly what you call completely tight. But, let me put it this way: They were never intended to deny an American constitutional rights, correct? That would be a misuse of those lists?

Mr. COMEY. I think that is fair to say. I hope that is true of all of our work.

Chairman JOHNSON. How do you get off of the lists?

Mr. COMEY. You get off of the list, either—and Nick will help me with this—but you get off of the list, either when an investigation has been closed, and then the agent sends the appropriate notification to have the name removed, or you make use of the redress procedures that DHS runs, to challenge and have it looked at—and then have your name removed if it is a mistake.

Chairman JOHNSON. Of course, you have to know that you are on the list in order to seek redress. And then, even there, that is not a judicial process, correct? That is just through the Agency. And, let us face it, a bureaucrat in the Agency will make the final determination. You do not have the ability to get redress through the courts.

Mr. COMEY. It is an administrative process, but people do and have gone to court to challenge it beyond that, as I recall.

Chairman JOHNSON. But, again, you have to know you are on the list.

Mr. COMEY. That is correct.

Chairman JOHNSON. That does represent a problem. And, again, I will understand if you do not want to speak to this in open session, but I think you have had some reservations about utilizing those, in terms of those lists tipping off someone that you may be investigating. Are you willing to speak to that at all?

Mr. COMEY. I think what I can say in open session is, I just want to be thoughtful about any operational impacts to anything that we set up.

Chairman JOHNSON. OK. My time is up. I am happy to let you respond to Senator Booker or—Senator Carper, do you have further questions?

Senator CARPER. I just want to yield my time to Senator Booker. Go ahead, please.

Senator BOOKER. Mr. Chairman, just for the record, it is ironic that I was asking a question about equal application of the law, and you did not equally apply the rules—if I can finish, sir. You, literally, even said to somebody, “Since there are only a few people here, I will let you go a little longer.” And right before—you seemed to be incredibly strict with your application of the rules to me—

Chairman JOHNSON. I cut other people off as well. Now, you can ask the question and get the answer.

Senator BOOKER. I would like, for the record¹, the details of how long people went over, so I can point out to the Chairperson how many minutes he allowed other people to go over—and then, when I am bringing up issues of race and equal application of the law, you suddenly cut me right off.

Chairman JOHNSON. That is an absurd characterization, but now you can get your answer.

Senator BOOKER. Sir, I am not a characterization. I would like that, for the record, at least, so you could see how you apply—how you are conducting the hearing, sir.

Director COMEY, I am going to finish the last paragraph of your speech that I did not read, going back, so I can heighten that issue of data.

“The first step to understanding what is really going on in our communities and in our country is to gather more and better data related to those we arrest, those we confront for breaking the law and jeopardizing public safety, and those who confront us. ‘Data’ seems a dry and boring word . . . without it, we cannot understand our world and make it better.”

Could you please comment on the lack of data, in regards to policing in the United States, and how hard it makes this to address the issue of implicit racial bias in policing?

Mr. COMEY. Yes, thank you, Senator Booker. This is one of the most important issues we confront in the FBI—I think we confront as Americans. There are all kinds of people of tremendously good hearts in law enforcement, not in law enforcement, and in communities of color, protesting. Every single one of them is unguided by actual data and information. Every conversation, in my view, about the use of force and race in policing, in this country, is uninformed—people of tremendous good will, trying to resolve these things.

What we could contribute, as a country, is information to that conversation, for the reasons you say, so that great people, who care deeply about these things, can come to solutions that are practical and just. We simply must collect data that is reliable, nationwide, about police use of deadly force in altercations—encounters with civilians. We simply must.

If there is anything more inherently governmental than that, I cannot imagine what it is. But, we are now in a situation, where we have newspapers that are the only source of that kind of data—and their data is not comprehensive.

¹ The information submitted by Senator Booker appears in the Appendix on page 88.

We are going to do this. I have spoken to—one of the beauties of a 10-year term is, I am not going to shut up about this. I have 7 years to go. We will build a nationwide database, which the FBI will collect, that can show us what happened when, who was involved, what were they like, and what were the circumstances—so we can have informed conversations.

No one in this country knows whether the use of deadly force against any particular group—African-Americans, most particularly—is up, down, or sideways, over the last 10 years. Nobody knows. Do we have an epidemic of violence? No one knows that. We could. We might not. We simply must gather the information, so we can care deeply, and solve these problems.

Senator BOOKER. Director Comey, I really celebrate your leadership around this issue—as was said—the courageous speech you gave, and your remarks, right now. But, the one thing I will ask you, sir, is: Where we do have data, it shows an alarming fact pattern in our country—not only the studies that you cite in your speech about implicit racial bias—but the Department of Justice has dozens and dozens of police departments, including the one that I ran—where I was even surprised at the data they collected—to begin to create transparency. So, police department after police department that has—where we do now have the data, it is showing very dramatic—from New York City, to New Orleans, to Ferguson—showing dramatic biases in policing.

So, does that not lead you to believe—or that you see this consistent fact pattern, where we have collected the data, that we do not just have a problem in the United States—to a Nation that aspires to high levels of justice and equality under the law—we do not have a policing crisis in this country, given the data that we do have?

Mr. COMEY. I believe we have a chasm in this country, in many places, where a divide is open—and opening between law enforcement and communities, especially the African-American community. The causes for it are complicated and longstanding, but not elusive. We can stare at it. We have problems—things we can do better in law enforcement that are obvious—and we are working very hard to change.

Where I think we can close the chasm is: Everybody wants the same kind of policing. Everybody does. Moms and dads as well as law enforcement want the same kind of policing—up close, responsible, lawful, and firm—but fair—policing—transparent. We are safer when we have it. And, the good news for America is, there are a ton of police leaders who feel exactly as I do. And, we are going to drive that chasm closer together, because it is the way to save lives in this country.

Senator BOOKER. And, I want to appreciate and highlight what you just said. As a guy who ran a police department, we have incredible police leaders out there—the overwhelming majority of whom seek the exact same thing as the black community—as other communities—and, frankly, who are undercelebrated on the level of daily heroism that they show in conducting their jobs, as I just mentioned, earlier in my testimony—in my questioning about the two Linden police officers. But, what people do not realize is that goes on every single day—there are people out there, putting them-

selves in harm's way, who do share our same values. But, what you so astutely pointed out—a lot of this is not conscious. Sometimes, people are not even aware of how they are not applying the law equally. And, when I see Justice Department investigation after Justice Department investigation, police departments large and small, and police departments run by African-Americans as well as white folks, all coming up with the same set of data—that is presenting the same fact: that we do not have the equal application of the law. When we have police—prisons that are now full of folks that—whether it is Vermont, where African-Americans are 1 percent of the population, but 11 percent of their prison population is African-American—or States like mine—this dramatic unequal application of the law, throughout the entire justice system—we have to get to the core of this understanding of what can we do to begin to correct for this implicit racial bias.

And, I will conclude with just saying that your prescription of having a better national collection of this data—we cannot get there unless we, first, engage in an objective, dispassionate analysis of the facts and the data. And, the fact that we do not collect them, 50 to 60 years after the Kerner Report, is outrageous and unacceptable.

Thank you.

Chairman JOHNSON. Thank you, Senator Booker. Senator Carper.

Senator CARPER. Mr. Chairman, just before we break up, we came here with a hearing in mind, concerning how we can better protect our homeland from threats, both foreign and domestic. And, I want to thank Senator Booker for adding something that I did not expect. And, I really want to say to Director Comey, thank you for the way you have engaged on what I think we all know is a really important subject.

We spent many months, in this room, years ago, on the heels of 9/11, with the 9/11 Commission, led by Lee Hamilton and Governor Kean. And, they had a vision that we would address and fix some of the problems that led to 9/11 and allowed it to happen. And, part of the problem was the stovepiping of information and our inability to work together and talk together. And, Mr. Comey, you said several times that we are not perfect—and the goal is to always be more perfect. I like to always cite the Preamble to the Constitution: “We the people of the United States, in order to form a more perfect union . . .” It does not say “in order to form a perfect union,” but “a more perfect union.” None of us are perfect. I always look at problems, and I say, “Find out what works, do more of that.” And, everything I do, I know I can do better. And, the same is true of all of us. But, I must say I am encouraged by the way you work together and the way your Agencies work together. And, I think we are all better for it.

And, as Jeh Johnson prepares to leave, in a couple months, for more fertile fields, maybe—I do not know—but I want to close, Mr. Chairman. The Chairman and I are baseball fans, and you may be as well. One of my favorite Detroit Tigers players was an outfielder named Kirk Gibson. And, when he had a memorable home run, playing for another team, for the Los Angeles Dodgers in a World Series, it sparked them to a World Series victory. But, years later,

he was back with the Tigers. In the middle of the season, he announces that he is going to retire—and he does it in a very different way. Usually, when people are going to retire from baseball, or whatever, they do it at the beginning of the season, or they do it in the middle of the winter, or they do it in spring training, and say, “I just do not have anything left anymore.” He did it in the middle of the season. And, he called the press corps to the Tiger dugout in July. And, he said, “I have an announcement to make. I have been traded.” And, people gasped. Then, he said, “Back to my family.”

So, Jeh, we are going to trade you back to your family, but you come with our best wishes and affection and our thanks to your wife, Susan, and to your family. God bless.

Chairman JOHNSON. Thank you, Senator Carper.

Again, I also would like to express my appreciation. I have, certainly, enjoyed working with Secretary Johnson. I think you have done a lot of good work, and you have hired some great people—and you have improved the Department. Thank you.

Gentlemen, thank you all for, again, your service to this Nation and for attending this hearing.

The hearing record will remain open for 15 days until October 12, at 5 p.m. for the submission of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 12:52 p.m., the Committee was adjourned.]

A P P E N D I X

Opening Statement of Chairman Johnson “Fifteen Years After 9/11: Threats to the Homeland” September 27, 2016

As submitted for the record:

Fifteen years have passed since September 11, 2001. Today, the threat of militant Islamic terrorist attacks to the United States remains significant.

Over the past year, Americans have suffered attacks inspired by Islamic Terrorism in San Bernardino, Orlando, Columbus, Philadelphia, and—most recently, the vicious attack in St. Cloud, Minnesota, and the bombings in New York and New Jersey.

In all, Islamic extremist terrorist have killed 63 people on U.S. soil since our committee last held its annual hearing to consider threats to the homeland and heard testimony from the heads of the FBI, DHS, and National Counterterrorism Center. And this does not count the horrific attacks that occurred in Paris, Brussels, and elsewhere across Europe, Africa, and the Middle East.

Two years after the President stated his goal of defeating ISIS, we have made little progress. As CIA Director Brennan told Congress in June, “our efforts have not reduced the group’s terrorism capability and global reach.” We need stronger American leadership.

There is no question that there are terrorists, rogue nations, and other criminal elements that want to harm this nation.

As Chairman of this Committee, through our hearings and oversight work, I have investigated vulnerabilities in our border, aviation, maritime, visa, cyber, and critical infrastructure security, and where possible I have worked on bipartisan legislation to address these threats.

Here is what I have learned about our nation’s vulnerabilities:

Our borders are not secure.

I am concerned that our system for vetting people coming to this country is not air tight, allowing potential adversaries to enter the country.

Federal agencies, and even components within DHS, are not always effectively working together—including in the aftermath of the San Bernardino attacks—which undermines our ability to prevent or respond to attacks.

Weaknesses remain in the security of our nation’s critical infrastructure and cybersecurity.

According to whistleblowers within DHS, I just learned that U.S. Citizenship and Immigration Services is working to naturalize as many citizens as possible before the election, rather than focusing on weaknesses in the current system that put our security at risk.

As Chairman of this Committee, I have worked to address these weaknesses, through oversight and bipartisan legislation. Our Committee has passed legislation to improve our border security, prevent human trafficking, enhance cybersecurity, and reform and strengthen Department of Homeland Security.

In all, we have passed 28 bills through our committee to improve our nation's security. Nine of these bills have become law and 11 have passed the Senate. Unfortunately, due to politics, some of our most important bills are being held up.

For example, our Committee has passed the DHS Accountability Act, which is significant reform legislation to improve the Department of Homeland Security. Today, I ask Secretary Johnson to publicly support our legislation, so that we can ask Senator Reid and others who are blocking the legislation to allow it to move forward to improve our nation's security.

I am concerned that the security threats facing our country are evolving and growing more serious by the day. We must all work together to continue addressing homeland security threats and strengthening our defenses. The American people are counting on us.

Statement of Ranking Member Tom Carper
“Fifteen Years After 9/11: Threats to the Homeland”
September 27, 2016

As prepared for delivery:

Mr. Chairman, thank you. We hold this hearing today on the heels of terrorist attacks in Minnesota, New Jersey, and New York. Thanks to the hard work and dedication of law enforcement officials, those attackers were identified and stopped before they could fully carry out their plans. The vigilance and quick thinking of everyday citizens likely saved many lives, as well. That alone serves as an important reminder that--if we see something, we need to say something.

While the investigations into these attacks and their specific motives are still being determined, it's clear that these attacks were carried out by two men - two Americans, in fact - who spent most of their lives in our country. These attacks underscore a key fact, the fact that the greatest threat to our homeland doesn't come from overseas. It doesn't come from Syrian refugees or from those who travel as tourists on the Visa Waiver program. The greatest threat to our country now comes from within -- from American citizens and legal residents who have spent most of their lives in this country. My colleagues and members of our staff may recall the words of renowned counter terrorism expert Peter Bergen who testified before this committee in November of last year when he said that, 'Every person who's been killed by a jihadi terrorist in this country since 9/11 has been killed by an American citizen or resident.'

Think about that. Many of these attacks are being carried out by Americans, by people who have lived here their entire lives or came here as children. They grew up knowing nothing else but life in America. Yet some have suggested that the way to stop these attacks is for America to ban entire groups of people from traveling to our country. Banning entire religious groups from entering the country will not prevent attacks from people like those committed by Ahmad Rahami in New York and New Jersey or Dahir Aden in Minnesota. Rahami came here at the age of 7, and Aden at the age of 2. They grew up here as Americans. I believe that those who would seal America's doors to immigrants and refugees fundamentally misunderstand how to stop these homegrown attacks.

The reality is that stopping homegrown terrorism starts with reaching out to local communities, building stronger partnerships, and making the American dream accessible to all. Fortunately, the Department of Homeland Security is doing just this with its Office of Community Partnerships. I am proud that this committee passed a bill with bipartisan support to enhance the ability of the Department to work with the Muslim community and others in order to counter the violent messages of ISIS and other terrorist organizations. Another important way to battle homegrown terrorism is by neutralizing the terrorists who create the hateful propaganda that is radicalizing our fellow Americans. That's why it's important that we keep taking the fight to ISIS. Simply put, we must continue to defeat and destroy this horrible terrorist group. By doing so, we prevent ISIS from portraying itself as a winner, and we bring to light the horrible abuses it thrusts upon innocent people of every age, race, religion, and nationality. The 60-nation coalition that we lead has put ISIS on the verge of defeat in Iraq and Syria.

For instance, ISIS once held more than 34,000 square miles in Iraq and Syria—an area the size of Austria. Over the past two years, we've taken back more than 50 percent of the land once held in Iraq, and more than 20 percent in Syria. Additionally, we've taken more than 45,000 ISIS fighters off the battlefield and drastically cut ISIS funding by a third. And thanks in part to the diligent efforts of our witnesses and the agencies they represent; we've significantly slowed recruitment of foreigners by ISIS from a high of about 2,000 a month in 2014 to 50 a month today. Not that long ago, roughly ten Americans per month were among those leaving home to join forces with ISIS. Today, that number has dropped to less than one per month. This battle is not over, but it's now clear that ISIS's days in Iraq and Syria are numbered. We need to make it clearer every day that ISIS is not the winning team that they present themselves to be. All of us have a role to play in making that clear to the American people, especially those who are susceptible to ISIS' siren song.

As we all know, the violent attacks ISIS inspires are not the only threat to our homeland. We also face the real threat that hackers and foreign intelligence services can attack and steal from us with a few clicks of a keyboard. As the frequency and variety of cyberattacks continues to increase, Congress has a responsibility to work with the federal government and the private sector to ensure they have the resources to continue addressing this evolving threat. Only by staying a step ahead of the threat can we ensure the security of our country online. Recent cyberattacks on American political organizations and state election systems have raised concerns regarding the threat posed by foreign governments attempting to interfere with the political process in the United States. Elections are the foundation of our democracy. And given the steps taken by state and local governments to secure our election systems, the American people should have confidence that their votes cannot be undermined by malicious actors or bullies from abroad.

With that being said, I think we can all agree that there is always room to improve. And when it comes to cybersecurity, lots of help is available. I want to commend Secretary Johnson and Director Comey for moving quickly to make assistance available to state and local officials to enhance the security of their election systems. This assistance is completely voluntary, and I hope states take advantage.

I would like to conclude by thanking all of our witnesses for being here and for their service to our country. For some of you, this may be the last time you appear before this Committee. So if I may, I'd like to just take moment to especially recognize Secretary Johnson for his leadership of the Department of Homeland Security. Secretary Johnson, I'd also like to thank you for making management reform one of your top priorities. As we saw with the most recent Federal Employee Viewpoint Survey, your efforts, along with those of Deputy Secretary Mayorkas and your leadership team, to improve morale are really paying off. While there is still more work to be done, I would like to commend you and your team for the significant boost in morale at the Department and all the improvements that you have made during your tenure. As we say in the Navy, 'Bravo Zulu.' Thank you again, Mr. Chairman, I look forward to a productive hearing.

Prepared Testimony

**Secretary of Homeland Security Jeh Charles Johnson
U.S. Senate
Committee on Homeland Security and Governmental Affairs**

“Fifteen Years after 9/11: Threats to the Homeland”**September 27, 2016**

Chairman Johnson, Senator Carper, and members of the Committee, thank you for holding this annual threats hearing with me, the FBI Director, and the Director of NCTC. I believe this annual opportunity for Congress to hear from us concerning threats to our homeland is important. I welcome the opportunity to be here again.

Counterterrorism

Today, 15 years after 9/11, it is still a dangerous world. Recent events in New York City, New Jersey, Minnesota, San Bernardino and Orlando are terrible reminders of the new threats we face to the homeland.

We have moved from a world of terrorist-directed attacks, to a world that also includes the threat of terrorist-inspired attacks – attacks by those who live among us in the homeland and self-radicalize, inspired by terrorist propaganda on the Internet, and terrorist-enabled attacks – those who are provided general guidance, such as potential targets, often in online conversations with terrorists overseas. By their nature, terrorist-inspired attacks and terrorist-enabled attacks are difficult to detect by our intelligence and law enforcement communities, could occur with little or no notice, and in general, make for a more complex homeland security challenge.

The events on September 17 illustrate the serious threat of homegrown violent extremism.

This threat environment has required a whole new type of response and we are aggressively strengthening and building more capabilities to respond.

As directed by President Obama, our government, along with our coalition partners, continues to take the fight militarily to terrorist organizations overseas. ISIL is the terrorist organization most prominent on the world stage. Since September 2014, air strikes and special operations have in fact led to the death of a number of ISIL's leaders and those focused on plotting external attacks in the West. At the same time, ISIL has lost about 49% of the populated areas it once controlled in Iraq, and thousands of square miles of territory it once controlled in Syria. But as ISIL loses territory, it has increased

UNCLASSIFIED

its plotting on targets outside of Iraq and Syria, and continues to encourage attacks in the United States.

On the law enforcement side, the FBI continues to, in my judgment, do an excellent job of detecting, investigating, preventing, and prosecuting terrorist plots here in the homeland.

Following the attacks in Ottawa, Canada in 2014, and in reaction to terrorist groups' public calls for attacks on government installations in the western world, I directed the Federal Protective Service to enhance its presence and security at various U.S. government buildings around the country.

The Department of Homeland Security has intensified our work with state and local law enforcement, and strengthened our information sharing efforts. Almost every day, we share intelligence and information with Joint Terrorism Task Forces, fusion centers, local police chiefs and sheriffs. And we are now able to instantly cross-reference suspects against law enforcement and counterterrorism databases and share information—often in almost real-time—with our domestic as well as international partners. We are also enhancing information sharing with organizations that represent businesses, college and professional sports, community and faith-based organizations, and critical infrastructure.

Since 2013 we've spearheaded something called the "DHS Data Framework" initiative. We are improving our ability to use DHS information for our homeland security purposes, and to strengthen our ability to compare DHS data with other travel, immigration, and other information at the unclassified and classified level. We are doing this consistent with laws and policies that protect privacy and civil liberties.

We also provide grant assistance to state and local governments around the country, for things such as active shooter training exercises, overtime for police officers and firefighters, salaries for emergency managers, emergency vehicles, and communications and surveillance equipment. We help to fund an active shooter training exercises such as those that took place in the New York City subways last November, a series of these exercises earlier this year in Miami and Louisville, and in June at Fenway Park in Boston. In February and June, we announced another two rounds of awards for FY 2016 that will fund similar activities over the next three years.

We are enhancing measures to detect and prevent travel to this country by foreign terrorist fighters.

We are strengthening the security of our Visa Waiver Program, which permits travelers from 38 different countries to come to the U.S. for a limited time period without a visa. In 2014, we began to collect more personal information in the Electronic System

for Travel Authorization, or “ESTA” system, that travelers from Visa Waiver countries are required to use. ESTA information is screened against the same counterterrorism and law enforcement databases that travelers with traditional visas are screened, and must be approved prior to an individual boarding a plane to the United States. As a result of these enhancements, since 2014, over 3500 additional travelers were denied visa-free travel here through this program. In August 2015, we introduced further security enhancements to the Visa Waiver Program.

Through the passage in December of the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015, Congress has codified into law several of these security enhancements, and placed new restrictions on eligibility for travel to the U.S. without a visa. We began to enforce these restrictions on January 21, 2016. Waivers from these restrictions have only been granted on a case-by-case basis, when it is in the law enforcement or national security interests of the United States to do so. Those denied entry under the Visa Waiver Program as a result of the new law may still apply for a visa to travel to the U.S. In February, under the authority given me by the new law, I also added three countries – Libya, Yemen and Somalia – to a list that prohibits anyone who has visited these nations in the past five years from traveling to the U.S. without a visa. In April, DHS began enforcing the mandatory use of high security electronic passports for all Visa Waiver Program travelers coming to the United States. In both February and June, CBP enhanced the ESTA application further with additional questions.

We are expanding the Department’s use of social media for various purposes. Today social media is used for over 30 different operational and investigative purposes within DHS. Beginning in 2014 we launched four pilot programs that involved consulting the social media of applicants for certain immigration benefits. USCIS now also reviews the social media of Syrian refugee applicants referred for enhanced vetting, and is extending this review to additional categories of refugee applicants. Based upon the recommendation of a Social Media Task Force within DHS, I have determined, consistent with relevant privacy and other laws, that we must expand the use of social media even further.

CBP is deploying personnel at various airports abroad, to pre-clear air travelers before they get on flights to the United States. At present, we have this pre-clearance capability at 15 airports overseas. And, last year, through pre-clearance, we denied boarding to over 10,700 travelers (or 29 per day) before they even got to the United States. As I said here last year, DHS intends to expand the pre-clearance program. In May 2015, I announced 10 additional airports in nine countries that we’ve prioritized for preclearance. In May 2016, CBP announced a new “open season,” running through August 1, for foreign airports to express interest in participating in the next round of preclearance expansion. Twenty-one airports submitted letters of interest. The Department is currently evaluating the submissions and I will make my determination this fall on which airports will participate in the next expansion. I urge Congress to pass

UNCLASSIFIED

legislation enabling preclearance operations in Canada, by providing legal clarity to CBP officials who are responsible for the day-to-day operation of preclearance facilities there.

For years Congress and others have urged us to develop a system for biometric exit – that is, to take the fingerprints or other biometric data of those who leave the country. CBP has begun testing technologies that can be deployed for this nationwide. With the passage of the FY 2016 Omnibus Appropriations Act, Congress authorized up to \$1 billion in fee increases over a period of 10 years to help pay for the implementation of biometric exit. In April, the Department delivered its Comprehensive Biometric Entry/Exit Plan to Congress, which details CBP's plan for expanding implementation of a biometric entry/exit system using that funding. I have directed that CBP redouble its efforts to achieve a biometric entry/exit system, and to begin implementing biometric exit, starting at the highest volume airports, in 2018.

Last January I announced the schedule for the final two phases of implementation of the REAL ID Act, which go into effect in January 2018 and then October 2020. At present, 24 states are compliant with the law, 28 states and territories have extensions, and four states and territories are out of compliance without an extension. Now that the final timetable for implementation of the law is in place, we urge all states, for the good of their residents, to comply with the law and start issuing REAL ID- compliant drivers' licenses and identification cards as soon as possible.

In the current threat environment, there is a role for the public too. "If You See Something, Say Something"™ must be more than a slogan. We continue to stress this. DHS has now established partnerships with the NFL, Major League Baseball and NASCAR, as well as with colleges and universities, to raise public awareness at sporting events and large gatherings. An informed and vigilant public contributes to national security.

In December we reformed "NTAS," the National Terrorism Advisory System. In 2011, we replaced the color-coded alerts with NTAS. But, the problem with NTAS was we never used it, it consisted of just two types of Alerts: "Elevated" and "Imminent," and depended on the presence of a known specific and credible threat. This does not work in the current environment, which includes the threat of homegrown, self-radicalized, terrorist-inspired attacks. So, in December we added a new form of advisory – the NTAS "Bulletin" – to augment the existing Alerts, and issued the first Bulletin providing the public with information on the current threat environment and how they can help. The December Bulletin expired in June, and we issued a new and updated Bulletin on June 15.

Given the nature of the evolving terrorist threat, building bridges to diverse communities is also a homeland security imperative. Well informed families and communities are the best defense against terrorist ideologies. Al Qaeda and ISIL are

targeting vulnerable communities in this country. We must respond. In my view, building bridges to our communities is as important as any of our other homeland security missions.

In 2015 we took these efforts to new levels. We created the DHS Office for Community Partnerships (OCP), which is now the central hub for the Department's efforts to counter violent extremism in this country, and the lead for a new interagency Countering Violent Extremism (CVE) Task Force that includes DHS, the Department of Justice (DOJ), the FBI, the National Counter Terrorism Center (NCTC) and other agencies. We are focused on partnering with and empowering communities by providing them a wide range of resources to use in preventing violent extremist recruitment and radicalization. Specifically, we are providing access to federal grant opportunities for state and local leaders, and partnering with the private sector to find innovative, community-based approaches.

Ensuring that the Nation's CVE efforts are sufficiently resourced has been an integral part of our overall efforts. On July 6, I announced the CVE Grant Program, with \$10 million in available funds provided by Congress in the 2016 Omnibus Appropriations Act. The CVE Grant Program will be administered jointly by OCP and FEMA. This is the first time federal funding at this level will be provided, on a competitive basis, specifically to support local CVE efforts. The funding will be competitively awarded to state, tribal, and local governments, nonprofit organizations, and institutions of higher education to support new and existing community-based efforts to counter violent extremist recruitment and radicalization to violence. The Department issued a notice of funding opportunity on July 6, formally announcing the grant program. Applications were due September 6, and the response has been overwhelming. We received over 200 applications and are currently in the review process.

Finally, I congratulate our personnel for another major accomplishment last week. Led by the U.S. Secret Service, literally thousands of DHS personnel were deployed to New York City for the security of the UN General Assembly. This was a massive undertaking involving over 100 visiting heads of state. This comes in the wake of their successful efforts to lead the protection of the Republican and Democratic National Conventions in Cleveland and Philadelphia July.

Aviation Security

As we have seen from recent attacks in Egypt, Somalia, Brussels, and Istanbul, the threat to aviation is real. We are taking aggressive steps to improve aviation and airport security. In the face of increased travel volume, we will not compromise aviation security to reduce wait times at Transportation Security Administration (TSA) screening check points. With the support of Congress we have surged resources and added personnel to address the increased volume of travelers.

UNCLASSIFIED

Since 2014 we have enhanced security at overseas last-point-of-departure airports, and a number of foreign governments have replicated those enhancements. Security at these last-point-of-departure airports remains a point of focus in light of attacks over the past year, including those in Brussels and Istanbul. By law, TSA is required to assess security at all foreign airports served by U.S. aircraft operators as well as foreign airports serving as last-point-of-departure locations. TSA conducts assessments at over 280 last-point-of-departure airports worldwide.

Last week, I represented the United States at a meeting of the United Nations Security Council, where we adopted the first-ever resolution on aviation security. In recognition of several significant international attacks on civil aviation this past year, the Security Council resolution calls on states to implement effective measures to mitigate threats and urges states to work with ICAO to support the effective implementation of international standards. The adoption of this UNSC resolution is an important step forward in the international community's commitment to aviation security and the advancement of global standards.

As you know, in May of last year a classified DHS Inspector General's test of certain TSA screening at eight airports, reflecting a dismal fail rate, was leaked to the press. I directed a 10-point plan to fix the problems identified by the IG. Under the new leadership of Admiral Pete Neffenger over the last year, TSA has aggressively implemented this plan. This has included retraining the entire Transportation Security Officers (TSO) workforce, increased use of random explosive trace detectors, testing and re-evaluating the screening equipment that was the subject of the IG's test, a rewrite of the standard operating procedures manual, increased manual screening, and less randomized inclusion in Pre-Check lanes. These measures were implemented on or ahead of schedule.

We are also focused on increasing other aspects of airport security, including restricting access to secure areas at airports. In April of last year TSA issued guidelines to domestic airports to reduce access to secure areas, to require that all airport and airline personnel pass through TSA screening if they intend to board a flight, to conduct more frequent physical screening of airport and airline personnel, and to conduct more frequent criminal background checks of airport and airline personnel. Since then employee access points have been reduced, and random screening of personnel within secure areas has increased four-fold. We have continued these efforts in 2016. In February, TSA issued guidelines to further enhance the screening of aviation workers in the secure area of airports, and in May, TSA and airport operators completed detailed airport-specific vulnerability assessments and mitigation plans for nearly 300 federalized airports.

We will continue to take appropriate precautionary measures, both seen and unseen, to respond to evolving aviation security threats and protect the traveling public.

UNCLASSIFIED

Without short-cutting aviation security, we are also working aggressively to improve efficiency and minimize wait times at airport security check points in the face of increased air travel volumes. I thank Congress for approving our three reprogramming requests this summer that have enabled us to expedite the hiring of over 1,300 new TSOs, pay additional overtime to the existing TSO workforce, convert over 2,700 TSOs from part-time to full-time.

We have also brought on and moved canine teams to assist in the screening of passengers at checkpoints, solicited over 150 volunteers from among the TSO workforce to accept temporary reassignment from less busy to busier airports, deployed optimization teams to the Nation's 20 busiest airports to improve operations, and stood up an Incident Command Center at TSA headquarters to monitor checkpoint trends in real time.

Airlines and airports also assisted in addressing wait times. We appreciate that major airlines and airport operators assigned personnel to certain non-security duties at TSA checkpoints, and provided support in a number of other ways.

Over the summer, the men and women of TSA worked hard to keep passengers moving through security checkpoints, and keep them safe. Their efforts paid off. Between May 25 and August 29 of this year, TSA screened over 200 million passengers and 98% of all passengers waited in line less than 30 minutes. In TSA Pre✓® lanes, 96% of passengers waited less than five minutes. Today, nationwide, the wait time for more than 98% of the traveling public is 30 minutes or less.

But we are not declaring victory. We plan to do more. We are preparing for the upcoming holiday travel season and will continue to work with Congress to ensure TSA has the resources it needs in the coming fiscal years.

Cybersecurity

Along with counterterrorism, cybersecurity remains a cornerstone of our Department's mission. Making tangible improvements to our Nation's cybersecurity is a top priority for President Obama and for me to accomplish before the end of the Administration.

I thank Congress for passing the Cybersecurity Act of 2015. This law is a huge asset to DHS and our cybersecurity mission and we are in the process of implementing it now. While I appreciate the additional authorities granted to us by Congress, I urge you to take further action and establish the Cyber and Infrastructure Protection Agency. The Cyber and Infrastructure Protection Agency would streamline and strengthen existing functions within the Department to ensure we are prepared for the growing cyber threat and the potential for large scale or catastrophic physical consequences as a result of an

attack. With the establishment of the Cyber and Infrastructure Protection Agency, DHS will be best positioned to execute our vital mission.

On February 9, the President announced his “Cybersecurity National Action Plan,” which is the culmination of seven years of effort by the Administration. The Plan includes a call for the creation of a Commission on Enhancing National Cybersecurity, additional investments in technology, federal cybersecurity, cyber education, new cyber talent in the federal workforce, and improved cyber incident response.

DHS has a role in almost every aspect of the President’s plan.

As reflected in the President’s 2017 budget request, we want to expand our cyber response teams from 10 to 48.

We are doubling the number of cybersecurity advisors to in effect make “house calls,” to assist private sector organizations with in-person, customized cybersecurity assessments and best practices.

Building on DHS’s “Stop. Think. Connect” campaign, we will help promote public awareness on multi-factor authentication.

I have also directed my team to focus urgently on improving our abilities to protect the Federal Government and private sector. Over the past year, the National Cybersecurity Communications Integration Center, or “NCCIC,” increased its distribution of information, the number of vulnerability assessments conducted, and the number of incident responses.

As required by the law, our NCCIC has built a system to automate the receipt and distribution of cyber threat indicators at real-time speed. We built this in a way that also includes privacy protections.

In March, I announced that this system was operational. At the same time, we issued interim guidelines and procedures, required by this law, providing federal agencies and the private sector with a clear understanding of how to share cyber threat indicators with the NCCIC, and how the NCCIC will share and use that information. We have now issued the final guidelines and procedures consistent with the deadline set by the law. We are now signing up companies and agencies to participate in this system.

I have issued an aggressive timetable for improving federal civilian cybersecurity, principally through two DHS programs:

The first is called EINSTEIN. EINSTEIN 1 and 2 have the ability to detect and monitor cybersecurity threats attempting to access our federal systems, and these protections are now in place across nearly all federal civilian departments and agencies.

EINSTEIN 3A is the newest iteration of the system, and has the ability to automatically block potential cyber intrusions on our federal systems. The Cybersecurity Act of 2015 requires federal civilian agencies to apply all available EINSTEIN protections to all information traveling into or out of their networks by the end of this year.

Thus far E3A has actually blocked over a million potential cyber threats, and we are rapidly expanding this capability. About a year ago, E3A covered only about 20% of our federal civilian networks. In the wake of the malicious cyber intrusion at the Office of Personnel Management, in May of last year I directed our cybersecurity team to make at least some aspects of E3A available to all federal departments and agencies by the end of last year. They met that deadline. Now that the system is available to all civilian agencies, 65% of federal personnel are actually protected, including the Office of Personnel Management, and we are working to get all large federal departments and agencies on board by the end of this year. We appreciate your continued support as we work to assist agencies meet their responsibility under the law during the next few months.

The second program, called Continuous Diagnostics and Mitigation, or CDM, helps agencies detect and prioritize vulnerabilities inside their networks. In 2015, we provided CDM sensors to all participating Federal agencies. Next year, DHS will provide the second phase of CDM to 100% of the federal civilian government.

I have also used my authorities granted by Congress to issue Binding Operational Directives and further drive improved cybersecurity across the federal government. In May 2015, I directed civilian agencies to promptly patch vulnerabilities on their Internet-facing devices. These vulnerabilities are accessible from the Internet, and thus present a significant risk if not quickly addressed. Agencies responded quickly and mitigated all of the vulnerabilities that existed when the directive was issued. Although new vulnerabilities are identified every day, agencies continue to fix these issues with greater urgency than before the directive.

In June I issued a second binding operational directive. This directive mandated that agencies participate in DHS-led assessments of their high value assets and implement specific recommendations to secure these important systems from our adversaries. We are working aggressively with the owners of those systems to increase their security.

In September 2015, DHS awarded a grant to the University of Texas at San Antonio to work with industry to identify a common set of best practices for the development of Information Sharing and Analysis Organizations, or "ISAOs." The

University of Texas at San Antonio recently released the first draft of these best practices. After public comment, they will be released in final form by September 30 and will be updated over the next year.

In recent months we have seen cyber intrusions involving political institutions and personal communications. We have also seen some efforts at cyber intrusions of voter registration data maintained in state election systems. We have confidence in the overall integrity of our electoral systems - it is diverse, subject to local control, and has many checks and balance built in. However, in this environment, we must be vigilant.

I have personally spoken with a number of state Secretaries of State, and DHS stands ready to assist state and local election officials in protecting their systems. In our cybersecurity mission, this is the nature of what we do – offer and provide assistance upon request. We do this for private businesses and other entities across the spectrum of the private and public sectors. DHS assistance is strictly voluntary and does not entail regulation, binding directives, and is not offered to supersede state and local control over the process. Our role is limited to support only.

We have offered the following services to state and election officials to assist in their cybersecurity: remotely conducted cyber hygiene scans on Internet-facing systems, risk and vulnerability assessments done on-site by DHS cybersecurity experts, access to the NCCIC 24x7 incident response center, sharing of relevant information on cyber incidents, sharing of best practices, and access to field-based cybersecurity advisors and protective security advisors. I am pleased that, to date, 18 states have requested our assistance. We will continue to strongly encourage more state and local election officials to do so.

Conclusion

I am pleased to provide the Committee with this overview of the progress we are making at DHS on countering threats. You have my commitment to work with each member of this Committee to build on our efforts to protect the American people.

I look forward to your questions.



Department of Justice

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

**BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
UNITED STATES SENATE**

**AT A HEARING ENTITLED
"15 YEARS AFTER 9/11: THREATS TO THE HOMELAND"**

**PRESENTED
SEPTEMBER 27, 2016**

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

**BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE**

**AT A HEARING ENTITLED
“15 YEARS AFTER 9/11: THREATS TO THE HOMELAND”**

**PRESENTED
SEPTEMBER 27, 2016**

Good afternoon Chairman Johnson, Ranking Member Carper, and members of the Committee. Thank you for the opportunity to appear before you today to discuss the current threats to the homeland and our efforts to address new challenges. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. Our successes depend on interagency cooperation; among those partners are with me today; the Department of Homeland Security and the National Counterterrorism Center to address current and emerging threats.

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists are extremely dynamic. The tragic event in Orlando last June is a somber reminder of this threat. The FBI is leading a Federal terrorism investigation with the assistance of our State, local, and Federal partners. The ongoing investigation has developed strong indications of radicalization by this killer, but further investigation is needed to determine if this attack was inspired by a foreign terrorist organization. We are spending a tremendous amount of time trying to understand every moment of the killer's path, to understand his motives, and to understand the details of his life. We will continue to look forward in this investigation, and backward. Our work is very challenging. We are looking for needles in a nationwide haystack, but we are also called upon to figure out which pieces of hay might someday become needles. That is hard work and the particular challenge of identifying homegrown violent extremists.

These threats remain the highest priority and create the most serious challenges for the FBI, the U.S. Intelligence Community, and our foreign, State, and local partners. ISIL is relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. 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. In addition, we are confronting an explosion of terrorist propaganda and training available via the Internet and social networking media. Due to online recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the U.S. to recruit and carry out acts. Terrorists in ungoverned spaces—both physical and cyber—readily disseminate poisoned propaganda and training materials to attract easily influenced individuals 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 and transformation from the terrorist threat our nation faced a decade ago. ISIL's widespread reach through the Internet and social media is most concerning as the group has proven dangerously competent at employing such tools for its nefarious strategy. ISIL uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Recently released propaganda has included various English language publications circulated via social media.

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.

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 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. Echoing other terrorist groups, ISIL has advocated for lone offender attacks in Western countries. Recent ISIL videos and propaganda specifically advocate for attacks against soldiers, law enforcement, and intelligence community personnel. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters. We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in

technology to their advantage. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States, including both physical and electronic surveillance. Physical surveillance is a critical and essential tool in detecting, disrupting, and preventing acts of terrorism, as well as gathering intelligence on those who are capable of doing harm to the nation. 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 pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the homeland.

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 two 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 new Intelligence Analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better prepared to work well together in the field. 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 what is directly in front of us. We must also be able to understand the threats we face at home and abroad and how those threats may be connected. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are 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 priority 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.

Cyber

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.

The pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber-attacks as a top priority. Within the FBI, we are targeting the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets. We need to be able to move from reacting to such attacks after the fact to operationally preventing such attacks. That is a significant challenge, but one we embrace. As the committee is well aware, the frequency and impact of cyber-attacks on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow.

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 last 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.

Another growing threat to businesses and individuals alike is Ransomware. Last year alone there was a reported loss of more than \$24 million. The FBI works closely with the private

sector so that companies may make informed decisions in response to malware attacks. Companies can prevent and mitigate malware infection by utilizing appropriate back-up and malware detection and prevention systems, and training employees to be skeptical of emails, attachments, and websites they don't recognize. The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity, lead to other victimizations, or be used to facilitate serious crimes.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and sharing inside and outside of government, to our internal emphasis on developing and retaining new talent and changing the way we operate to evolve with the cyber threat. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States from all of those threats and the men and women of the Bureau continue to meet and exceed those expectations, every day. I want to thank them for their dedication and their service.

Chairman Johnson, Ranking Member Carper, and Committee members, I thank you for the opportunity to testify concerning the threats to the Homeland. I am happy to answer any questions you might have.

**Hearing before the Senate Homeland Security and Governmental Affairs Committee
"Fifteen Years after 9/11: Threats to the Homeland"**

September 27, 2016

**Nicholas J. Rasmussen
Director
National Counterterrorism Center**

Thank you, Chairman Johnson, Ranking Member Carper, and Members of the Committee. I appreciate this opportunity to discuss the terrorism threats that concern us most. I am pleased to join my colleagues and close partners, Secretary Jeh Johnson from the Department of Homeland Security (DHS), and Director James Comey of the Federal Bureau of Investigation (FBI).

During the past several years, we have had great success in strengthening our Homeland security and have made progress in reducing external threats emanating from core al-Qa'ida and the self-proclaimed Islamic State of Iraq and the Levant, or ISIL, due to aggressive counterterrorism (CT) action against the groups. Unfortunately, the range of threats we face has become increasingly diverse and geographically expansive, as we saw with ISIL's wave of attacks this summer in Bangladesh, Iraq, France, Germany, Saudi Arabia, and Turkey. As these attacks demonstrate, ISIL's strategy is to weaken the resolve of its adversaries and project its influence worldwide through attacks and propaganda, ultimately perpetuating fear.

The continuing appeal of the violent extremist narrative and the adaptive nature of violent extremist groups continue to pose substantial challenges to the efforts of our CT community. In addition to the attacks overseas, homegrown violent extremists, or HVEs, who are inspired by groups such as ISIL remain an unpredictable threat we face in the Homeland. Because HVEs are frequently lone actors, often self-initiating and self-motivating, their threats are harder to detect and, therefore, harder to prevent. But just as the threat evolves, so do we. We are constantly adapting, and we must continue to improve.

Threat Overview

Recent events, to include the knife attack earlier this month in Minnesota and IED detonations and recoveries in New York and New Jersey, underscore the importance of the intelligence community (IC) and law enforcement vigilance against terrorism in the Homeland. While the FBI continues to investigate these attacks, and as we learn more about the circumstances surrounding those attacks and the suspects involved, they demonstrate the ongoing threat we face from individuals who choose relatively simple attack methods, in some cases using readily available instructions on the internet or propagated by terrorist organizations. As I've noted in previous sessions with this Committee, the IC and our law enforcement partners face a persistent challenge in detecting HVEs who may be motivated by an array of factors and who in some cases may also suffer from mental health issues. Recent attacks continue to inform how we detect and respond to these types of incidents, and we remain committed to keeping our Nation safe. The best way to combat terrorism is a whole-of-government approach, where federal, state, and local intelligence and law enforcement collaborate.

We expect some HVEs will try to replicate the violence and potentially capitalize on the media coverage that recent attacks have generated. Although we do not see a large number of these types of threats at

the moment, we expect to see an increase in threat reporting around the upcoming election and the transition period between November and January. We will continue to track and monitor the threats and share that information with our partners.

In the past few years, the pool of potential HVEs has expanded. As Director Comey has previously said, the FBI has investigations on approximately 1,000 potential HVEs across all fifty states. While HVEs have multiple factors driving their mobilization to violence, this increase in caseload tracks with ISIL's rise in prominence and its large-scale media and propaganda efforts to reach and influence populations worldwide. What we have seen over time is that HVEs—either lone actors or small insular groups—tend to gravitate toward simple tactics that do not require advanced skills or outside training. We expect that most HVEs will likely continue to select traditional targets, such as military personnel, law enforcement, and other symbols of the US government, although during the past year we have seen HVEs plotting against softer civilian targets as was the case in St. Cloud, Minnesota, in the Chelsea neighborhood in Manhattan, and in Seaside Park, New Jersey most recently. Some HVEs—such as the Orlando shooter in June and the San Bernardino shooters in December 2015—may have conducted attacks against personally significant targets. The convergence of violent extremist ideology and personal grievances or perceived affronts likely played a role in motivating these HVEs to attack. We are still working to learn more about what may have motivated the suspects in the attacks in Minnesota, and in New York and New Jersey.

Having passed the 15-year mark since 9/11, the array of terrorist actors around the globe is broader, wider, and deeper than it has been at any time since that day. ISIL's narrative, rooted in unceasing warfare against all enemies, extends beyond the Syria-Iraq battlefield. ISIL has conducted attacks ranging in tactics and targets—the bombing of a Russian airliner in Egypt; the attacks in Paris at restaurants, a sports stadium, and a concert venue; the killing of hostages and law enforcement officials at a café in Bangladesh; and the bombing of a crowded commercial district in Baghdad—all of which demonstrate how ISIL can capitalize on local networks on the ground for attacks. The threat landscape is less predictable and, while the scale of the capabilities currently demonstrated by most of these violent extremist actors does not rise to the level that core al-Qa'ida had on 9/11, it is fair to say that we face more threats originating in more places and involving more individuals than we have at any time in the past 15 years.

As we saw this summer at Istanbul's Ataturk Airport and with the attack in Belgium in March, terrorists remain focused on aviation targets because they recognize the economic damage that may result from even unsuccessful attempts to down aircraft or against airline terminals, as well as the high loss of life and the attention media devotes to these attacks. Worldwide security improvements in the aftermath of the 9/11 attacks have hardened the aviation sector but have not entirely removed the threat. Violent extremist publications continue to promote the desirability of aviation attacks and have provided information that could be used to target the air domain.

We have come to view the threat from ISIL as a spectrum, where on one end, individuals are inspired by ISIL's narrative and propaganda, and at the other end, ISIL members are giving operatives direct guidance. Unfortunately, the gradations on that spectrum are not always distinct; sometimes ISIL members in Iraq and Syria reach out to individuals in the Homeland and elsewhere to conduct attacks on their behalf. More often than not, we observe a fluid picture where individuals operate somewhere between the two extremes.

ISIL's access to resources—in terms of both manpower and funds—and territorial control in areas of Syria and Iraq are the ingredients that we traditionally look to as being critical to the group maintaining an external operations capability, to include ISIL's ability to threaten the Homeland. For that reason,

shrinking the size of territory controlled by ISIL, and denying the group access to additional manpower and funds in the form of foreign fighters and operatives as well as oil revenue and other financial resources, remains a top priority, and success in these areas will ultimately be essential to our efforts to prevent the group from operating as a terrorist organization with global reach and impact. And clearly, progress has been made in these areas: ISIL has lost over half its territory in Iraq and nearly a quarter in Syria; the number of fighters it has in those countries is significantly down, and its illicit income streams are down. But despite this progress, it is our judgment that ISIL's ability to carry out terrorist attacks in Syria, Iraq, and abroad has not to date been significantly diminished, and the tempo of ISIL-linked terrorist activity is a reminder of the group's continued global reach.

While ISIL's efforts on the ground in Syria and Iraq remain a top priority for the group's leadership, we do not judge that there is a direct link between the group's current battlefield status in Iraq and Syria and the group's capacity to operate as a terrorist organization with global capabilities. Their external operations capability has been building and entrenching during the past two years, and we do not think battlefield losses alone will be sufficient to completely degrade the group's terrorism capabilities. As we have seen, the group has launched attacks in periods when it held large swaths of territory as well as when under significant pressure from the counter-ISIL campaign. In addition to its efforts to conduct external attacks from its safe havens in Iraq and Syria, ISIL's capacity to reach sympathizers around the world through its robust social media capability is unprecedented and gives the group access to large numbers of HVEs.

This year, ISIL has lost several key leaders who have been with the group for years – most recently ISIL spokesman and external operations leader Abu Muhammad al-Adnani and ISIL's minister of information Wail Salman – whose deaths deprive the group of senior ranking members with unique skillsets. Adnani's final public statement encouraged ISIL supporters in the US to conduct attacks at home instead of traveling to Iraq and Syria, suggesting that ISIL recognizes the difficulty in sending operatives to the Homeland for an attack. ISIL likely views the US as a harder target than Europe due to Europe's proximity to the conflict. US ports of entry are also under far less strain from mass migration, and US law enforcement agencies are not overtaxed by persistent unrest, as are some of our counterparts overseas.

In Europe, we are concerned about ISIL's demonstrated ability to conduct coordinated attacks by deploying operatives from Syria and Iraq and by leveraging Europe-based individuals who have responded to ISIL's call to act on the group's behalf. ISIL attacks in Paris in November and Brussels in March revealed several factors that could enable future operations. First, the role of ISIL's cadre of foreign fighters in planning and executing external operations is key. As we know, several of the Paris and Brussels attackers had experience fighting in Syria, including Paris attack coordinator and operative Abdelhamid Abaaoud.

A second factor that has contributed to ISIL's successful attacks in Europe is the flexibility of its operatives. Those serving as facilitators can transition to attackers for different operations. Some of the Brussels attackers supported the Paris attacks by providing explosives and transportation for operatives. This is a dynamic that the US Government must consider in order to effectively aid our European counterparts in identifying and disrupting future attacks. Finally, ISIL's leveraging of criminal, familial, and communal ties contributes to its ability to advance plotting in Europe. Many operatives involved in the attacks in Paris and Brussels share a similar story of getting involved in criminal activities before becoming radicalized to violence.

Last year we confirmed that ISIL had successfully sent several operatives—including at least two of the Paris attackers—from Syria to Western Europe by having them blend in with the flow of some 1 million migrants, asylum seekers, and refugees who traveled from Turkey to Greece in 2015. Although ISIL most

likely will continue to seek opportunities to infiltrate these Europe-bound flows when it is operationally expedient to do so, the group probably would prefer other options to deploy operatives to the Homeland because of the relative difficulties in entering the US via the US Refugee Admissions Program. Specifically, applicants have little-to-no control as to whether the UN will refer them for consideration by the US Refugee Admissions Program. Those refugees who are referred by the UN to the US Refugee Admissions Program are then subjected to the US Government's process for refugee resettlement, including the most stringent security screening process for any type of traveler to the US. .

To ensure proper scrutiny of refugee applicants referred to the US by the UNHCR, the National Counterterrorism Center (NCTC) has worked extensively with the screening community to deliver a comprehensive, end-to-end refugee vetting system that streamlines operations without compromising safety, removes stovepipes, and increases transparency across the board. This screening is just one part of a robust system of checks—that involves the Department of Homeland Security, FBI, and State Department, Defense Department, as well as other intelligence agencies—that includes extensive in-person overseas interviews, biographic and biometric assessments, and recurrent vetting.

NCTC screening is done in two ways: The first is identity resolution. We utilize automated programs to correlate biographic information of refugee applicants against the Terrorist Identities Datamart Environment, the US Government's central repository of international terrorist information, for potential matches. All of these computer-generated matches are reviewed by analysts trained to resolve identities. We access other IC holdings to then validate those findings. The second step is screening against IC CT holdings. We screen applicant biographic information against these holdings to identify possible matches to intelligence reporting and then conduct further analysis to determine any nexus to terrorism.

The tremendous efforts we are undertaking to counter the ISIL threat are absolutely warranted, but I want to stress that we still view al-Qa'ida and the various al-Qa'ida affiliates and nodes as a principal counterterrorism priority. For example, while ISIL is driving most terrorist threats against Europe, we know that the pressures we face on the Continent are not limited to ISIL. The attack on the *Charlie Hebdo* magazine office in Paris by individuals linked to al-Qa'ida in the Arabian Peninsula in January 2015 is a key example of the broad violent extremist threat facing Europe. We would not tier our priorities in such a way that downgrades al-Qa'ida in favor of a greater focus on ISIL. When we are looking at the terrorism threats that we face as a nation, including to the Homeland, al-Qa'ida still figures prominently in that analysis.

We are particularly concerned about al-Qa'ida's safe haven in Syria because we know al-Qa'ida is trying to strengthen its global networks by relocating some of its remaining leadership cadre from South Asia to Syria. These leaders include some who have been part of the group since before the September 11 attacks and, once in Syria, we believe they will work with the al-Qa'ida affiliate there—the Nusra Front—to threaten the US and our allies.

The Nusra Front is al-Qa'ida's largest affiliate and one of the most capable armed groups operating in Syria. Its integration of al-Qa'ida veterans provides the group with strategic guidance and enhances its standing within the al-Qa'ida global movement. We believe the Nusra Front's July statement announcing the separation of the group from the broader al-Qa'ida movement is in name only and that Nusra Front will remain part of al-Qa'ida, supporting its ideology and intent to target the West, as it has since its covert founding as a front for al-Qa'ida in Iraq in 2012. We will remain vigilant in our efforts to counter this group and the threats it poses to the West.

We believe we have constrained al-Qa'ida's effectiveness and its ability to recruit, train, and deploy operatives from its safe haven in South Asia; however, this does not mean that the threat from core al-Qa'ida in the tribal areas of Pakistan or in eastern Afghanistan has been eliminated. We assess that al-Qa'ida and its adherents in the region still aspire to conduct attacks and, so long as the group can potentially regenerate capability to threaten the Homeland with large-scale attacks, al-Qa'ida will remain a threat. Al-Qa'ida's allies in South Asia—particularly the Haqqani Taliban Network—also continue to present a high threat to our regional interests.

The IC is cognizant of the level of risk the US may face over time if al-Qa'ida regenerates, finds renewed safe haven, or restores lost capability. We are very much on alert for signs that al-Qa'ida's capability to attack the West from South Asia is being restored and would warn immediately if we find trends in that direction. I am confident that the US Government will retain sufficient capability to continue to put pressure on that core al-Qa'ida network and therefore reduce the risk of a resurgence by al-Qa'ida in the region.

We also see increasing competition between violent extremist actors within South Asia itself, between and among the Taliban, ISIL's branch in South Asia, and al-Qa'ida. This is an additional dynamic that we are working to understand. While conflict among terrorist groups may well distract them from their core mission of plotting attacks against Western targets, conflict also serves to introduce a degree of uncertainty into the terrorism landscape that raises questions that I don't think we have answers to yet. This is something we are watching very closely.

Stepping back, there are two trends in the contemporary threat environment that concern us most. First is the increasing ability of terrorist actors to communicate with each other outside our reach with the use of encrypted communications. As a result, collecting precise intelligence on terrorist intentions and the status of particular terrorist plots is increasingly difficult.

There are several reasons for this: exposure of intelligence collection techniques, disclosures of classified information that have given terrorist groups a better understanding of how we collect intelligence, and terrorist groups' innovative and agile use of new means of communicating, including ways that are sometimes beyond our ability to collect, known as "going dark."

Second, while we've seen a decrease in the frequency of large-scale, complex plotting efforts that sometimes span several years, we're instead seeing a proliferation of more rapidly evolving threat or plot vectors that emerge simply by an individual encouraged to take action who then quickly gathers the few resources needed and moves into an operational phase. The so-called "flash-to-bang" ratio—the time between when an individual decides to attack and when the attack occurs—in plotting of this sort is extremely compressed and allows little time for traditional law enforcement and intelligence tools to disrupt or mitigate potential plots.

ISIL is aware of this, and those connected to the group have understood that by motivating actors in their own locations to take action against Western countries and targets, these actors can be effective, especially if they cannot travel abroad to ISIL-controlled areas. In terms of propaganda and recruitment, ISIL supporters can generate further support for their movement, even without carrying out catastrophic, mass-casualty attacks. And that's an innovation in the terrorist playbook that poses a great challenge. Further, martyrdom videos and official ISIL claims of responsibility for inspired individuals' attacks probably allow the group to convey a greater impression of control over attacks in the West and maximize international media exposure.

Countering Violent Extremism (CVE)

The number of individuals going abroad as foreign terrorist fighters to Iraq and Syria only emphasizes the importance of prevention. Any hope of enduring security against terrorism or defeating organizations like ISIL rests in our ability to counter the appeal of terrorism and dissuade individuals from joining them in the first place.

To this end, as announced in January 2016, the Countering Violent Extremism Task Force was stood up to organize federal CVE efforts. The CVE Task Force is being led by the Department of Homeland Security for the first two years; afterward, the Department of Justice will assume leadership. It is being staffed by multiple departments and agencies, including the FBI and NCTC. The main objectives of the task force are to coordinate federal support for ongoing and future research, and establish feedback mechanisms to incorporate sound results; synchronize federal government outreach to, and engagement with, CVE stakeholders and provide technical assistance to CVE practitioners; manage and leverage digital technologies to engage, empower, and connect CVE stakeholders; and work with CVE stakeholders to develop intervention programs.

NCTC continues to refine and expand the preventive side of counterterrorism. We have seen a steady proliferation of more proactive and engaged community awareness efforts across the US, with the goal of giving communities the information and tools they need to see violent extremism in their midst and do something about it before it manifests itself. NCTC, in direct collaboration with DHS and the inter-agency team, has led the creation of CVE tools to build community resilience across the country.

NCTC has sent our officers on multiple occasions to meet with the communities in places such as Denver, Sacramento, Buffalo, and Minneapolis to raise awareness among community and law enforcement audiences about the terrorist recruitment threat. Our briefing is now tailored to address the specific issue of foreign fighter recruitment in Syria and Iraq, and we have received a strong demand signal for more such outreach. The Community Resilience Exercise, a tabletop exercise that brings together local law enforcement with community leadership to run through a hypothetical case-study-based scenario featuring a possible violent extremist or foreign fighter, aims to encourage the creation of intervention models at the local level. In the same way that local partners, including law enforcement, schools, social service providers, and communities, have come together to provide alternative pathways and off-ramps for people who might be vulnerable to joining a gang, we are encouraging our local partners to implement similar models for violent extremism. The more resilient the community, the less likely its members are to join a violent extremist group.

Conclusion

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for the opportunity to testify before you this morning. The role that NCTC, FBI, and DHS play in combating terrorism, along with this Committee's support, is critically important. I know the collaboration among all the agencies represented here will continue during the months and years to come to continue to protect the Homeland.

Thank you all very much, and I look forward to answering your questions.

U.S. DEPARTMENT OF STATE - PRODUCED TO HOCR
NOT FOR PUBLIC RELEASE
C06125520 UNCLASSIFIED U.S. Department of State Case No. O-2016-11097 Doc No. C06125520 Date: 09/08/2016

RELEASE IN PART B6

Re: Question

From: Colin Powell [REDACTED]
To: Hillary Clinton hr15@att.blackberry.net
Subject: Re: Question

B6

I didn't have a BlackBerry. What I did do was have a personal computer that was hooked up to a private phone line (sounds ancient.) So I could communicate with a wide range of friends directly without it going through the State Department servers. I even used it to do business with some foreign leaders and some of the senior folks in the Department on their personal email accounts. I did the same thing on the road in hotels.

Now, the real issue had to do with PDAs, as we called them a few years ago before BlackBerry became a noun. And the issue was DS would not allow them into the secure spaces, especially up your way. When I asked why not they gave me all kinds of nonsense about how they gave out signals and could be read by spies, etc. Same reason they tried to keep mobile phones out of the suite. I had numerous meetings with them. We even opened one up for them to try to explain to me why it was more dangerous than say, a remote control for one of the many TVs in the suite. Or something embedded in my shoe heel. They never satisfied me and NSA/CIA wouldn't back off. So, we just went about our business and stopped asking. I had an ancient version of a PDA and used it. In general, the suite was so sealed that it is hard to get signals in or out wirelessly.

However, there is a real danger. If it is public that you have a BlackBerry and it is government and you are using it, government or not, to do business, it may become an official record and subject to the law. Reading about the President's BB rules this morning, it sounds like it won't be as useful as it used to be. Be very careful. I got around it all by not saying much and not using systems that captured the data.

You will find DS driving you crazy if you let them. They had Maddy tied up in knots. I refused to let them live in my house or build a place on my property. They found an empty garage half a block away. On weekends, I drove my beloved cars around town without them following me. I promised I would have a phone and not be gone more than an hour or two at Tysons or the hardware store. They hated it and asked me to sign a letter relieving them of responsibility if I got whacked while doing that. I gladly did. Spontaneity was my security. They wanted to have two to three guys follow me around the building all the time. I said if they were doing their job guarding the place, they didn't need to follow me. I relented and let one guy follow me one

UNCLASSIFIED U.S. Department of State Case No. O-2016-11097 Doc No. C06125520 Date: 09/08/2016

U.S. DEPARTMENT OF STATE - PRODUCED TO HOCR
NOT FOR PUBLIC RELEASE
C06125520 UNCLASSIFIED U.S. Department of State Case No. O-2016-11097 Doc No. C06125520 Date: 09/06/2016

full corridor behind just so they knew where I was if I was needed immediately. Their job is to keep you hermetically sealed up. Love, Colin

On Fri, Jan 23, 2009 at 7:37 AM, > wrote:
Dear Colin,

I hope to catch up soon w you, but I have one pressing question which only you can answer!
What were the restrictions on your use of your blackberry? Did you use it in your personal office? I've been told that the DSS personnel knew you had one and used it but no one fesses up to knowing how you used it!
President Obama has struck a blow for berry addicts like us. I just have to figure out how to bring along the State Dept. Any and all advice is welcome.
All the best to you and Alma, Hillary

UNCLASSIFIED U.S. Department of State Case No. O-2016-11097 Doc No. C06125520 Date: 09/06/2016

U.S. DEPARTMENT OF STATE - PRODUCED TO HOCR
NOT FOR PUBLIC RELEASE
C06125521 UNCLASSIFIED U.S. Department of State Case No. O-2016-11097 Doc No. C06125521 Date: 09/06/2016

RELEASE IN PART B6

Re: Question

To: Colin Powell [REDACTED]

Subject: Re: Question

B6

Colin, I am finally out of the SCIF and want to thank you for all of the advice about berries, security and life on the 7th floor! I hope we'll have a chance to visit in person sometime soon. All the best, H

UNCLASSIFIED U.S. Department of State Case No. O-2016-11097 Doc No. C06125521 Date: 09/06/2016

**Question Round Timing
for September 27, 2016, HSGAC hearing**

Time stamps according to video:

<http://www.hsgac.senate.gov/hearings/fifteen-years-after-9/11-threats-to-the-homeland>

Senator	Round 1	Round 2	Round 3
Johnson	37:10-45:48	2:15:21-2:21:52	2:46:07-2:53:04
Carper	45:55-54:27	2:21:59-2:31:42	3:00:21-3:02:47
Paul	54:57-1:02:33	--	--
McCaskill	1:02:35-1:09:37	--	--
Ayotte	1:09:54-1:17:15	--	--
Tester	1:17:16-1:24:30	--	--
Booker	1:24:36-1:31:10	2:38:50-2:45:53	2:53:14-3:00:18
Peters	--	2:31:45-2:38:44	--
Baldwin	1:31:17-1:38:45	--	--
Portman	1:38:51-1:46:31	--	--
Sasse	1:46:33-1:54:11	--	--
Ernst	1:54:12-2:01:26	--	--
Heitkamp	2:01:28-2:07:12	--	--
Lankford	2:07:16-2:15:17	--	--

Question round in minutes:

Senator	Round 1	Round 2	Round 3	Total
Johnson	8:38	6:31	6:57	22:06
Carper	8:32	9:43	2:26	20:41
Paul	7:36	--	--	7:36
McCaskill	7:02	--	--	7:02
Ayotte	7:21	--	--	7:21
Tester	7:14	--	--	7:14
Booker	6:34	7:03	7:04	20:41
Peters	--	6:59	--	6:59
Baldwin	7:28	--	--	7:28
Portman	7:40	--	--	7:40
Sasse	7:38	--	--	7:38
Ernst	7:14	--	--	7:14
Heitkamp	5:44	--	--	5:44
Lankford	8:01	--	--	8:01



**CWS Statement to the Senate Committee on Homeland Security & Governmental Affairs,
pertaining to its hearing on Tuesday, September 27, 2016**

As a 70-year old humanitarian organization representing 37 Protestant, Anglican and Orthodox communions and 33 refugee resettlement offices across the United States, Church World Service (CWS) urges all Members of Congress to affirm the importance of the current U.S. refugee resettlement program and uphold robust protections for asylum seekers and other vulnerable individuals fleeing persecution and violence. We know from sacred texts across faith traditions that nations will be judged by how they treat the most vulnerable: the widow, the orphan, the refugee, during trying times.

To be considered a refugee, individuals must prove that they have fled persecution due to their nationality, ethnicity, religion, political opinion or membership in a particular social group. Refugees face three options: return to their home country, integrate in the country to which they first fled, or be resettled to a third country. For the millions who are unable to return home due to significant threats to their safety and rejection by the country to which they first fled, resettlement is the last resort. As we face the largest displacement crisis in recorded history, with over 65 million displaced persons worldwide, less than one percent of the world's estimated 21.3 million refugees are resettled to a third country. As one of 28 countries that resettles refugees, the U.S. Refugee Admissions Program (USRAP) is a public-private partnership that helps rescue refugees who have no other means of finding safety, prioritizing refugees who are especially vulnerable.

Security measures are intrinsic to the integrity of the U.S. refugee resettlement program, which is the most difficult way to enter the country. Refugees are the most vetted individuals to enter the United States. Every refugee undergoes biographic and bio-metric checks; medical screenings; DNA testing for family reunification cases; in-person interviews by Department of Homeland Security (DHS) officials, and interagency checks with DHS, the Federal Bureau of Investigation, Department of State, Department of Defense, and National Counterterrorism Center. Mandatory supervisory review of all decisions; random case assignment; inter-agency national security teams; trained document experts; forensic testing of documents; and interpreter monitoring make the U.S. refugee screening process the more thorough in the world. Due to technological advances, refugees from Syria are also undergoing iris scans to confirm their identity.

Similarly, the United States already has rigid national security procedures in place for asylum applicants in accordance with our obligations under international¹ and domestic² immigration laws. Asylum seekers in the United States include women, men, and children who are religious minorities persecuted for their beliefs; trafficked for commercial sex or forced labor; and human rights defenders who have worked against oppressive regimes around the world. Existing procedures are already in place to ensure the integrity of the U.S. asylum system, as well as important safeguards to prevent individuals from being returned into harm's way. For example, arriving asylum seekers are subject to mandatory biographic and biometric checks reviewed against various federal databases by well-trained fraud detection officers.

The United States has a tightly regulated asylum system that, despite backlogs and shortfalls in access to legal counsel, allows people fleeing persecution to have their cases heard and evaluated by immigration adjudicators. For example, Sami³ fled Iraq and sought asylum in the United States because he was targeted by terrorists for supplying water to American service camps. He repeatedly received death threats, and on at least two occasions, extremists accosted his family, once breaking his son's arm and leaving Sami unconscious in a remote part of the desert. He, his wife, and children are practicing Chaldean Catholics, a religious minority in Iraq that has been persecuted for centuries — often, churches in and around Sami's community are burned. Sami had no choice but to leave. They began the long, at times dangerous, journey, through Europe to Central America, and finally up through Mexico to the U.S. border. They presented themselves to Border Patrol agents asking for help, at which point they were detained. Eventually, he and his family were granted asylum.

Today, it is paramount that the U.S. refugee resettlement program and asylum system remain true to their mission to protect the most vulnerable individuals who face persecution and violence. Economic studies show that all immigrants provide substantial contributions to the workforce and to local economic development. Congress should strengthen access to protections for refugees, asylum seekers, and immigrants, all of whom contribute to their new communities with their innovative skills, dedicated work, and inspiring perseverance.

CWS is strongly opposed to any efforts to dismantle or curtail the current U.S. refugee resettlement program or U.S. asylum system. CWS urges all Members of Congress to recognize the life-saving importance these programs, as families flee torture, violence, and other human rights abuses simply because of who they are and what they believe. Let us reflect the best of our nation by extending hospitality and leading by example so that other nations do the same.

¹ The Convention on the Rights of the Child, Articles 2, 3, 6 and 22. www.ohchr.org/en/professionalinterest/pages/crc.aspx; The Universal Declaration of Human Rights, Article 14. www.un.org/en/documents/udhr/index.shtml#14; United Nations General Assembly, Declaration on Territorial Asylum, 14 December 1967, A/RES/2312(XXII). www.refworld.org/docid/3b0065a2.html; United Nations High Commissioner for Refugees, A Framework for the Protection of Children www.unhcr.org/50f6d0b9.html; United Nations High Commissioner for Refugees, Convention and Protocol Relating to the Status of Refugees. www.unhcr.org/3b66c2aa.html.

² Immigration and Nationality Act § 208, 8 U.S.C. § 1157.

³ Not his real name.

**Post-Hearing Questions for the Record
Submitted to Hon. Jeh C. Johnson
From Senator Claire McCaskill**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

Question#:	1
Topic:	Implausible Events
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to a question for the record after the April 14, 2016 Homeland Security and Governmental Affairs (HSGAC) hearing, the Department of Homeland Security (DHS) defined "plausible" as follows: "of all possible terrorist activities within the chemical-biological-radiological-nuclear (CBRN) threat space, plausible designates a higher probability of occurrence vs. other events." Based on that definition of what is "plausible," it is possible that DHS could be comparing 2 incredibly unlikely events, and one of them will always be more likely than the other to occur, so DHS is going to be spending countermeasure funding no matter what. In other words, at a time when federal funding is tight, DHS is defining "plausible" in such a way as to guarantee that we spend money on something, even if it's a Black Swan, 1-in-a-billion chance event.

If it is the case that DHS determines that a threat is plausible because of its higher probability of occurrence than other events, then, by definition, DHS must have decided that some events are "improbable" and countermeasures are not necessary.

Please provide a list of events that DHS has determined to be "implausible" and has decided to take no action on nor recommend the procurement of countermeasures to HHS?

Response: The Department of Homeland Security (DHS) remains concerned about the enduring risk of chemical, biological, radiological, and nuclear (CBRN) threats. The consequences of these attacks are potentially high even though the likelihood of their occurrence is relatively low.

While the probability of occurrence of any scenario is one important factor in determining the appropriate level of preparation for CBRN threats, the level of consequence is also a critical factor which must be considered in determining the appropriate level of preparatory investment and action. In light of this, we use our

Question#:	1
Topic:	Implausible Events
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

current understanding of the threat and potential pathways, such as dispersion of anthrax spore in a subway, introduction of a toxin in processed food, chemical release in a shopping mall, etc. to continually assess which capabilities to fund, and to what levels, through our resource allocation process.

DHS is able to define the risk of CBRN threats by conducting rigorous Terrorism Risk Assessments (TRAs).¹ Each assessment defines risk as a function of likelihood of a terrorist conducting a successful attack, and the consequences of that attack, should one occur. The results of these assessments are a relative ranking of potential terrorist events involving Weapons of Mass Destruction (WMD).

DHS does not consider the likelihood of a terrorist nuclear threat as “implausible.” The Radiological and Nuclear Terrorism Risk Assessment analyzes the entire spectrum of radiological or nuclear threats. Given the tremendous human and economic consequences that would result from a successful radiological or nuclear terrorist attack, DHS does not advocate that countermeasures are unnecessary for any threat or scenario involving radiological or nuclear terrorism which we analyze.

In addition to CBRN Terrorism Risk Assessments, DHS conducts Material Threat Assessments (MTAs) which assess the threat posed by given CBRN agents and the potential number of human exposures in plausible high-consequence scenarios.

¹ These assessments, which are classified, are in response to Homeland Security Presidential Directives (HSPD) 10 (Biodefense), 14 (Domestic Nuclear Detection), 18 (Medical Countermeasures against Weapons of Mass Destruction (WMD)) and 22 (Chemical Defense). DHS conducts a Chemical, Biological, Radiological and Nuclear, and an Integrated Terrorism Risk Assessment.

Question#:	2
Topic:	Material Threat Determination
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Ebola countermeasures are a perfect example of how this definition of "plausible" can result in wasteful spending. BioShield money is supposed to be used only for preparation against bioterror events. Yet somehow weaponized Ebola is on DHS's list of material threats, despite near-unanimous scientific agreement that it cannot be successfully weaponized.

In QFRs, DHS said that "the concern with Ebola has its foundation in the U.S. and Soviet Union's biological weapons programs of the Cold War Era," and DHS remains concerned about weaponized Ebola even though, "neither country was successful in achieving their goals with this pathogen." DHS went on to admit that they, "remain worried about this virus because of the amount of press it has received during the past several years." DHS also states that, "[s]cenarios exist for the introduction of Ebola in the U.S. via a terrorist act," but that such an event is "unlikely."

How much, if at all, do scientific consensus and public sentiment factor into the plausibility analysis of a particular threat or the determination to issue a material threat determination?

Response: The Terrorism Risk Assessments (TRAs) depend heavily on scientific data in the analysis of all WMD threat agents, and scientific consensus is sought for all of the data used to support the modeling effort. While input from the general scientific community is exceptionally valuable and incorporated in our analyses, it often offers limited insight into the potential consequences of a terrorist event involving the intentional use of WMD to damage the homeland. Because the U.S. ended its cold-war era biological weapons program and destroyed all samples, data, and information when we became a signatory to the Biological Weapons Convention (BWC) in 1972, and because the Ebola virus was not discovered until 1976 after the U.S. program was ended, there is a dearth of knowledge on the ability for Ebola and related Filoviruses to be used as instruments of terror. In the absence of data that addresses the unique aspects that differentiate a naturally occurring disease and that caused by an intentional act of terrorism, it cannot be unequivocally said that they cannot be weaponized.

Most important in the risk assessments produced by DHS is data provided by the intelligence and law enforcement communities' information on terrorist interest, capabilities, and intention. When combined with the scientific information informing estimates of consequences, the results form the foundation for recommendations. It is "unlikely" that a terrorist will successfully conduct an attack involving Ebola virus. However, in our analysis, Ebola virus is more likely to be used in a terror event than

Question#:	2
Topic:	Material Threat Determination
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

other agents considered in the analysis. More importantly, the consequences of an attack involving Ebola could be graver than those of many other biological hazards. As a result, based on the likelihood of a successful attack, the consequence of a successful attack, and the combination of those two factors, DHS determined that the Ebola virus represents a material threat to national security, and we recommend vigilance. As our research programs generate the data necessary to answer fundamental questions regarding the potential of Ebola and other Filoviruses to be used as weapons to damage the homeland, DHS has and will update our recommendations to the public health community.

Question#:	3
Topic:	Plausible Biothreats
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The fact that DHS is spending millions of dollars earmarked specifically for bioterror threats on an implausible event based mostly on public sentiment (rather than rigorous analysis) and Cold War-era concerns that have since been debunked demonstrates a complete lack of adherence to its own policies and any realistic, fact-based process for spending these federal funds.

I understand that we were in the middle of a crisis with Ebola, and it is plausible that HHS and DHS were just looking for any possible funding during the crisis. If that is the case, maybe we need to be having a policy discussion about whether Bioshield money should be reserved exclusively for bioterrorist events or should be broadly available for all biothreats, whether man-made or naturally occurring. Otherwise, if DHS really is going to take the position that weaponized Ebola continues to be a bioterror threat, then DHS's analytical models badly need to be reviewed and reconsidered because there is no rational explanation for spending bioterror money on Ebola.

Based on this analysis, which do you believe is a more appropriate course of action going forward: does DHS continue to believe that weaponized Ebola is a "plausible" scenario, does DHS need to take a hard look at the process, or should DHS and lawmakers be discussing some changes to the BioShield Act to allow DHS and HHS to better prioritize spending for the most plausible biothreats, including potentially naturally occurring biothreats like Zika, Ebola, and the Tularemia outbreak in Colorado last year?

Response: The purpose of Project BioShield is to accelerate the research, development, purchase, and availability of effective medical countermeasures against chemical, biological, radiological, and nuclear (CBRN) agents. Before the Department of Health and Human Services (HHS) may use Project BioShield funds to purchase security countermeasures against CBRN agents, the Secretary of Homeland Security must make a determination that a CBRN agent is a material threat sufficient to affect national security. Following this determination, the Secretary of HHS is required to assess the potential public health consequences for the U.S. population of exposure to the material threat agent, determine whether countermeasures are necessary to protect the public health, assess the availability and appropriateness of specific countermeasures to address the material threat, and determine which countermeasures are appropriate for the Strategic National Stockpile as required by the BioShield Act of 2004.

Additionally, DHS' role is further defined in Section 302 of the Homeland Security Act of 2002 as "developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies

Question#:	3
Topic:	Plausible Biothreats
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats..." In its statutory role, DHS focuses on intentional acts that may plausibly be perpetrated by a terrorist, and has not included naturally occurring and emerging public health threats like Zika virus in our risk assessments. Based on available information, DHS determined that Ebola virus, among many other potential biological agents, represented a material threat to national security. This determination authorized, though it did not compel, late-stage development by HHS and potential procurement by it of medical countermeasures to address that particular threat. Ongoing refinement of our analyses continued to support the conclusion that Ebola virus represents a material threat to the national security based on the likelihood of an attack and consequences of an attack should a successful attack occur. As our research programs generate the data necessary to answer fundamental questions regarding the potential of Ebola and other filoviruses to be used as weapons to damage the homeland, DHS will update our recommendations to the public health community.

Question#:	4
Topic:	Technical Performance Requirements
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS continues to deploy Gen-2 BioWatch detectors, and even these Gen-2 BioWatch machines are of questionable utility. GAO found that, "DHS lacks reliable information about BioWatch Gen-2's technical capabilities to detect a biological attack, in part, because in the 12 years since BioWatch's initial deployment, DHS has not developed technical performance requirements for Gen-2."

Is DHS planning to develop technical performance requirements, and, if so, what is the expected date of completion of these requirements? Without these requirements, does it make sense to continue spending money to deploy a technology that has no performance requirements?

Response: The BioWatch Program's detection capabilities have been independently tested and validated by 4 testing events conducted over the last 6 years, including testing in a laboratory, in a controlled environment, and in an open air environment. The results of these testing events reinforced the Department's assessment of the system's ability to perform the mission for which it was intended: detecting a large-scale aerosol release of specific threat agents in our most populous cities. BioWatch provided test reports, including results, to the GAO.

DHS S&T and BioWatch are collaborating to advance a plan for enhancing BioWatch technologies to increase coverage and speed of detection. These improvements are intended to advance the current "detect to treat" capability, which will further enable us to deploy medical countermeasures before the population is symptomatic. BioWatch and the DHS S&T developed a Technology Road Map outlining near-term (1-3 years) and mid- to long-term (3+ years) BioWatch technology enhancements with an estimated deployment of near-term enhancements in Fiscal Year 2018, pending appropriated funding.

BioWatch in collaboration, with DHS S&T, has been proceeding with the technology acquisition in accordance with DHS Acquisition Management Directives and Instructions. As part of the acquisition process, BioWatch will develop an Operational Requirements Document (ORD) and a Concept of Operations (CONOPs) document by the end of Fiscal Year 2017. These documents will include a set of realistic and viable performance requirements for the enhancements to the BioWatch system. Throughout this effort, DHS will use system-level metrics as the basis for translating between detection system/subsystem technical requirements (and demonstrated performance) and the ability of future enhanced biodetection systems to achieve the program's operational objectives.

Question#:	5
Topic:	Holistic Thinking
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Another problem with Gen-2 is that it was designed to detect only aerosolized bio-attacks, so any naturally-occurring outbreak will go undetected, even if a natural event is more likely to occur. In Colorado in 2015, for example, an outbreak of tularemia went undetected by Gen-2 machines there because the outbreak was a naturally-occurring event. Again, we seem to be so focused about the threat of terrorism that we're missing the more likely and more serious threats that can occur naturally.

Does the federal government need to start thinking more holistically about the threats we face and how we prepare for them?

Response: Yes, while bioterrorism remains a high priority, the Department of Homeland Security (DHS) agrees that a more holistic approach to biodefense is an important goal. DHS is in the process of enhancing our capabilities to be more flexible in the types of biological threats and hazards that can be detected.

Even though the current BioWatch system (referred to as Gen-2) was designed to detect a large-scale aerosolized biological threat, the system has shown that it is capable of detecting evidence of naturally occurring organisms of interest in the environment, even when they exist at very low levels. In the example you reference, BioWatch did in fact detect *Francisella tularensis* (causative agent of tularemia) in Colorado during 2015 and 2016.

During that time period, the BioWatch Program analyzed over 237,000 samples from across all BioWatch jurisdictions; of them, 7 yielded detections of *Francisella tularensis* that met the algorithm necessary for a BioWatch Actionable Result (BAR) declaration. This paralleled the clinical diagnosis of tularemia being observed in the Denver human and rodent populations.

Question#:	6
Topic:	TSA Whistleblower Protection
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In June, I asked Admiral Neffenger about whistleblower retaliation at TSA, and in QFRs I asked what specific steps he had taken to change the culture within senior management at TSA and make clear that retaliation will not be tolerated.

In response, Adm. Neffenger could only point to one specific action he has taken, citing new guidance on directed reassignments, but on nothing else. Instead his response was a general commitment to investing in TSA employees, treating them with respect and protecting their due process rights.

Compounding this seeming inaction on whistleblower protections is an apparent lack of accountability for senior management, too. When I asked Admiral Neffenger whether anyone was held accountable for the security failures after covert airport security tests by the DHS Inspector General when the IG was able to get 67 of 70 illegal items through airport security, and the man in charge of TSA security at the time was also found to have skirted federal bonus laws and got \$90,000 in bonuses the same year as these tests, the response I got was that "no single individual can be held accountable for an organizational failure."

Do you agree with that statement? If so, how can we hold anyone accountable?

Please provide a proposal with specific action items to improve accountability and reduce whistleblower retaliation at TSA.

Response: I would refer you to Administrator Neffenger for further elaboration of his responses to your questions. However, I would note generally that his appointment as TSA administrator was once of the important senior management changes made in response to the screening failures identified in last year's OIG report.

With respect to whistleblower matters, TSA takes any allegations of retaliation seriously and fully cooperates with any U.S. Office of Special Counsel (OSC) or DHS Office of Inspector General (OIG) investigation. All newly hired TSA employees must complete a mandatory course regarding their rights and remedies available under employment discrimination and whistleblower protection laws, as set forth in the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 ("No FEAR Act"). TSA employees complete the training within 90 days of employment and every two years thereafter. In Fiscal Year 2016, 97.4 percent of TSA employees (64,659 individuals) completed this training. TSA's Office of Inspection investigators have received additional training specific to their responsibilities when investigating whistleblower

Question#:	6
Topic:	TSA Whistleblower Protection
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

disclosures. Further, all TSA supervisors must take the OSC Prohibited Personnel Practices/Whistleblower Disclosure Training, a course developed by OSC in conjunction with DHS and released in August of 2016. As of October 2016, the completion rate for this course is 96.7 percent, with the goal of ensuring 100 percent of TSA's supervisory personnel complete the training by the end of the year.

TSA encourages employees to voice their views through a variety of avenues and strongly supports employee disclosures of perceived violations of law or gross mismanagement to the OIG or the OSC. TSA also continues to review current policies and procedures to make certain personnel and administrative policies are appropriately crafted, clearly stated, and followed in practice. TSA and DHS are committed to protecting the rights of employees who report what they reasonably believe are violations of laws, rules, or regulations; gross mismanagement; gross waste of funds; abuse of authority; or substantial and specific danger to public health and safety. Working with employees and citizens, the Department, OIG and OSC, TSA endeavors to protect the integrity, effectiveness and efficiency of all its programs.

Question#:	7
Topic:	Retaliation Findings
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: When I asked Admiral Neffenger in a QFR for the number of number of whistleblower retaliation findings within TSA in the last 5 years, he responded that "neither OSC nor any federal court has made a finding of whistleblower retaliation with respect to any senior executives at TSA." Yet the New York Times reported that OSC had obtained corrective actions for 7 TSA employees who claimed retaliation in 2015 alone.

Please provide the total number of instances in the past 5 years where corrective actions were obtained by a whistleblower employee of TSA either through actions taken by OSC, a federal district court or the DHS IG, and any corresponding actions taken against the alleged retaliator. If no actions were taken against the retaliator, please provide a reason for taking no action. All information can be provided without personally identifiable information as needed.

Response: The previous Question For the Record asked: "In the past 5 years, how many senior executives at TSA have been found guilty of retaliation against whistleblowers by the IG, OSC, or a federal court?" In the past five years, U.S. Office of Special Counsel (OSC) has not made any finding of whistleblower retaliation with respect to any senior executive at the Transportation Security Administration (TSA). There are no TSA cases where corrective action was obtained by the Department of Homeland Security Office of Inspector General (DHS OIG) in the past five years, and TSA has never had a whistleblower retaliation finding in U.S. district court.

In the last five years, OSC has provided one draft report to TSA finding that two employees were subjected to retaliation. The management official involved in that case was not a senior executive. This case was resolved when the management official took a demotion and the two employees received corrective action including withdrawal of a Performance Improvement Plan, a proposed 14-day suspension, a mentorship agreement and a Letter of Reprimand, and issuance of retroactive in-position increases, performance appraisals and performance awards. Over the past five years, eight other complaints filed with OSC were resolved through settlement agreements. At the time of these agreements, there were no findings made by OSC regarding these cases and the agreements did not constitute an admission or acknowledgment of any wrongdoing by either the Agency or the employee.

Additionally, there were also actions taken outside of OSC, a federal district court or the DHS OIG. There were two adverse decisions from the Merit Systems Protection Board (MSPB) ordering corrective action. In one of these cases, TSA's Office of Professional

Question#:	7
Topic:	Retaliation Findings
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Responsibility is considering potential disciplinary action against the manager. In the other case, TSA took no action against the managers named in the appeal, and OSC declined to pursue discipline against the managers following the MSPB's decision.

Over the past five years, 13 other MSPB appeals regarding whistleblower retaliation were resolved through settlement agreements. At the time of these agreements, there were no decisions made by MSPB regarding these cases and the agreements did not constitute an admission or acknowledgment of any wrongdoing by either the Agency or the employee.

**Post-Hearing Questions for the Record
Submitted to Hon. Jeh C. Johnson
From Senator Jon Tester**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

Question#:	8
Topic:	Communication Across the Northern Border
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Jon Tester
Committee:	HOMELAND SECURITY (SENATE)

Question: You had mentioned prior knowledge to gaps in communication between federal law enforcement officers across the northern border.

To the degree that you are able to discuss this in an unclassified setting, what actions is DHS taking to remedy this? Does DHS have plans to assist CBP in the acquisition process in order to build up communication infrastructure for our first responders along the northern border? I would also like to request that your office brief my staff on this gap in communication to the greatest extent possible in a TS-level brief.

Response: Interoperability is a concern of the entire Homeland Security Enterprise, which means it depends on collaboration among federal, state, local, and tribal agencies. In that context, the Department of Homeland Security’s (DHS) role is to facilitate and encourage opportunities for interoperability. We do that through our state and local liaisons and the DHS Office of Science and Technology First Responder Group.

Within DHS, our emphasis is on ensuring our systems include interoperability as part of their requirements, design, and implementation. For example, our Joint Wireless Program Management Office (JWPMO) includes interoperability in all requirements definition and system acquisition activities, which allows us to integrate readily with state, local, tribal, international, and other parties as our combined commitment to interoperability evolves and matures.

On March 10, 2016, the Under Secretary for Management signed the *DHS Interoperable Communications Act Strategic Plan* as required by the DHS Interoperable Communications Act, Public Law 114-29 (July 6, 2015). The Under Secretary for Management issued Policy Directive 034-04, *Joint Wireless Interoperability Program Tactical Communications*, in support of that strategy on July 22, 2016.

Question#:	8
Topic:	Communication Across the Norther Border
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Jon Tester
Committee:	HOMELAND SECURITY (SENATE)

In addition to these efforts, under the 2011 Beyond the Border Declaration and Action Plan announced by President Obama and former Prime Minister Harper, Canada and the United States agreed to implement a binational radio interoperability system between border law enforcement personnel to (1) better coordinate responses to border incidents and investigations and (2) improve officer and public safety. CBP is currently conducting pilots of the program in Vermont, Michigan, and Washington State, which will explore how radio interoperability technology can be deployed across the Northern Border in new locations. These pilots will run until July 2017.

The Department will coordinate with the appropriate officials to schedule a briefing with your staff.

Question#:	9
Topic:	Social Media Task Force Recommendations
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Jon Tester
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you mention taking the recommendations of the Social Media Task Force within DHS.

What recommendations from this Task Force are a priority for you while you are still Secretary of DHS?

Response: DHS's Social Media Task Force recommended and I approved creating a centralized, department-wide social media screening and vetting capability. The development of an automated screening and vetting capability, and a properly resourced structure to oversee, coordinate, and facilitate Department efforts to expand social media screening and vetting use across DHS mission sets is a Department priority. Additionally, centralization will allow the Department to continually develop and refine social media tools while also codifying and sharing best practices for social media screening and vetting.

Question#:	10
Topic:	Reassessment of National Security Policies
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Jon Tester
Committee:	HOMELAND SECURITY (SENATE)

Question: In the aftermath of 9/11, we saw the creation of new departments and agencies, including DHS and NCTC, as well as new standards, policies, and procedures throughout the executive and legislative branches.

Do you believe that we need another assessment of our national security policies, from top-to-bottom, just as the Hart-Rudman Commission did?

In your opinion, are structural changes to our government's national security apparatus needed?

Response: Our overall challenge within the Department of Homeland Security, and within the homeland security community of the federal, state and local governments of this Nation, is to learn from and adapt to the changing character of the evolving threats and hazards we face. Accordingly, the Department recurrently assesses national security policies and procedures to ensure we are open and transparent about our policies and decision-making processes. One way DHS does this, is through the Quadrennial Homeland Security Review (QHSR), required by the Implementing Recommendations of the 9/11 Commission Act of 2007, which is a comprehensive examination of the homeland security strategy of the Nation conducted every four years. The QHSR process assesses and may make recommendations to address authorities, missions, policies, programs, capabilities, and budget priorities.

As for structural changes needed at DHS, we appreciate last year's successes and the assistance provided by the Congress – in particular, the Cybersecurity Act of 2015 and funding for CVE efforts, as well as the overall funding of DHS for Fiscal Year 2016.

However, we believe additional legislation is needed to authorize and institutionalize the significant progress DHS has made over the past several years in management reform and multi-component operations. This will ensure that the incoming Secretary has the tools needed to manage the Department of Homeland Security effectively from Day One.

These management reform efforts, which are part of the Unity of Effort initiative I launched in 2014, focus on eliminating stove pipes where it makes sense, improving operational effectiveness, and promoting transparency. We have encouraged Congress to formally codify many of the changes made through this initiative in legislation.

**Post-Hearing Questions for the Record
Submitted to Hon. Jeh C. Johnson
From Senator Tammy Baldwin**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

Question#:	11
Topic:	Increased Grant Funding
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Tammy Baldwin
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you discussed grant assistance that DHS provides to local governments. These programs are essential in providing first responders with the training and resources they need. I am concerned that we may need more resources given the increase in attacks on soft targets.

For example, the Milwaukee fusion center, The Southeastern Wisconsin Threat Analysis Center, worked with the FBI to prevent a terrorist attack in my home state earlier this year and does extensive work to prevent crime and acts of terrorism on a regular basis. Unfortunately, the center had to reduce its full time personnel by two-thirds when Milwaukee no longer qualified for UASI funding under the risk formula. The center could use additional funding to protect vulnerable areas in the city, and I am sure other jurisdictions are in need of training and resources in this threat environment as well.

Given the increase in attacks on soft targets across the country and in communities large and small, would you agree there is a need for increased grant funding to states and local jurisdictions?

How is the threat portion of the formula evolving in light of the uptick in soft target attacks and have you considered expanding eligibility?

Response: The President’s Fiscal Year 2017 budget proposal reflects difficult decisions among competing priorities across the DHS portfolio. The proposed cuts to the preparedness grants programs give consideration to the \$47.7 billion in funding appropriated to preparedness grants in the 15 years since the 2001 terrorist attacks and the significant progress made in building preparedness across the nation during that timeframe. As funding for grant programs began to decline in Fiscal 2012, the Department emphasized that state and local governments should use their grant funding to sustain the capabilities they built over the past 15 years with federal grant funding

Question#:	11
Topic:	Increased Grant Funding
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Tammy Baldwin
Committee:	HOMELAND SECURITY (SENATE)

rather than invest in new capabilities that are more costly and will be difficult to sustain in the future.

The proposed FY 2017 budget includes an allocation of \$330 million for the Urban Area Security Initiative (UASI), which represents a \$270 million (45%) reduction compared to the \$600 million allocated for FY 2016. However, the Administration is proposing \$100 million for a new Regional Competitive Grant Program which will target critical capability gaps at the regional level. As the funds would be awarded on a competitive basis, with regional risk mitigation being the primary focus, the highest risk urban areas will likely benefit most from this program. Similarly, urban areas will benefit from the \$49 million that is proposed for Countering Violent Extremism programs and activities targeted at preventing, preparing for, and responding to complex, coordinated terrorist attacks. The additional funding through these supplemental programs, coupled with an emphasis on sustaining existing capabilities, will help ensure that the metropolitan areas at highest risk will receive the future resources they need.

The Threat portion of the overall risk formula focuses on Intelligence Community (IC) reporting related to a specific geographic area or state, not the specific targets that may be located within their boundaries. The infrastructure located within these areas is addressed in the vulnerability and consequence sections of the Risk Assessment. The Department of Homeland Security, Office of Intelligence & Analysis's (I&A) threat analysis considers specific, implied and potential physical terrorist threats reported in IC reporting and FBI information. The threat assessment includes IC disseminated threat reporting that revealed known and credible violent extremist plots, casings, threats, or aspirations, as well as reviews of significant terrorism-related incidents within areas.

Further, on June 16, 2016, the Department of Homeland Security issued a National Threat Advisory System (NTAS) bulletin, highlighting that the homeland is currently facing a dynamic threat environment from homegrown violent extremists, who by their nature operate individually or in small groups with little to no observable indicators of nefarious activity. In light of this threat environment, this year, the threat analysis conducted by the Office of Intelligence and Analysis was broadened to reflect the nature of homegrown violent extremism by acknowledging that almost all Metropolitan Statistical Areas could potentially be targeted by homegrown violent extremists previously unknown to law enforcement and the Intelligence Community. This approach is more indicative of the current threat that the Nation faces.

For Fiscal Years 2015 and 2016, the Joint Explanatory Statements which accompanied the Department of Homeland Security's appropriations acts contained language directing the Department to limit funding within the Urban Area Security Initiative (UASI)

Question#:	11
Topic:	Increased Grant Funding
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Tammy Baldwin
Committee:	HOMELAND SECURITY (SENATE)

program to those cities comprising the top 85 percent of total identified nationwide risk. This limitation, while not affecting the methods used to determine an urban area's relative risk, did set a definite limit on the number of urban areas selected as UASI sites for each of those fiscal years.

Question#:	12
Topic:	Protecting Personally identifiable information
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Tammy Baldwin
Committee:	HOMELAND SECURITY (SENATE)

Question: Cybersecurity is one of the most complex challenges we face. I firmly support strong cybersecurity efforts and giving federal agencies the tools they need to keep us safe from harm. At the same time, I believe that it is equally important that we ensure the privacy of law-abiding Americans. In your testimony, you reference the Cybersecurity Act of 2015, which passed in last year's omnibus. I did not support a version of this legislation as a standalone bill, but I did support the year-end Omnibus.

Specifically, I had concerns with the breadth of information that DHS would receive under the overly broad definition of "cyber threat indicator," the weak rules on companies to remove personally identifiable information and the requirement for DHS to automatically disseminate these indicators.

How is DHS protecting personally identifiable information throughout the cyber threat indicator sharing process and how it is handling un-scrubbed data?

Response: DHS has taken careful measures to ensure privacy and civil liberties protections are fully implemented in the automated indicator sharing (AIS) capability and regularly tested. To avoid over-collection, AIS uses submission guidance and specific technical instructions, consistent with the definitions provided by the Cybersecurity Act of 2015, which limits the amount and type of data to that which is directly related to cyber threats. Most of the data fields are technical in nature, and not related to the potential collection of personally identifiable information (PII). In the limited instances where a data field may include PII, AIS has processes, including a "privacy scrub", which perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat; incorporate elements of human review on select fields of certain indicators that might possibly contain PII to ensure that automated processes are functioning appropriately; minimize the amount of data included in a cyber threat indicator to information that is directly related to a cyber threat; retain only information needed to address cyber threats; and ensure any information received is used only for network defense or limited law enforcement purposes. Analysts conducting human review are trained in the handling of PII. DHS does not retain or share un-scrubbed data and deletes any PII that is not directly related to a cyber threat upon processing.

In order to receive protections afforded by the Cybersecurity Act of 2015, participants are required to follow AIS submission guidance that outlines the type of information that should and should not be provided when submitting indicators through AIS. Specifically, the guidance instructs AIS participants that the indicators they submit should not include PII unless it is directly related to the cybersecurity threat. Regardless of who the

Question#:	12
Topic:	Protecting Personally identifiable information
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Tammy Baldwin
Committee:	HOMELAND SECURITY (SENATE)

participant is, every indicator goes through the "privacy scrub" described above. DHS does not share un-scrubbed data and deletes any PII that is not directly related to a cyber threat upon processing.

In March 2016, the Department published a Privacy Impact Assessment of AIS that details how we mitigate privacy risks. Final procedures and guidelines for AIS, including Privacy and Civil Liberties, were published by the Departments of Homeland Security and Justice in June 2016. These documents can be found online at: <https://www.us-cert.gov/ais>.

Question#:	13
Topic:	Preventing Hate Crimes
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Tammy Baldwin
Committee:	HOMELAND SECURITY (SENATE)

Question: I am deeply concerned by the repeated attacks against various vulnerable populations in this country - the LGBT community, religious minorities, particular racial and ethnic groups - just to name a few. We held a hearing a just few months ago about the horrific tragedy in Orlando. While this was an act inspired by terrorist groups and a terrible incident of gun violence, it was also a hate crime targeting the LGBT and Latino communities. That is why I have been working to bolster federal efforts to prevent bias-motivated violence and enforce federal civil rights and hate crime laws through the Department of Justice.

What is the Department of Homeland Security doing to prevent hate crimes and bias-motivated attacks in its counterintelligence work?

Response: The DHS Office for Civil Rights and Civil Liberties (CRCL) leads the Department's nation-wide engagement efforts with diverse communities including, but not limited to, religious minorities, the LGBTQ community, and various ethnic communities. The engagement program is designed to share reliable information with community stakeholders on federal, state, and local governments' programs and initiatives; obtain feedback on government policies; provide avenues of redress and address community grievance; and deepen the channels of communication between government agencies and community stakeholders.

Specifically, following the Orlando nightclub tragedy, CRCL activated and hosted an Incident Community Coordination Team (ICCT) call on Monday, June 13, 2016, to share information on available resources and address concerns and questions from community stakeholders. The ICCT is a cross-sector, interest based coordinated effort to bring together Federal, state, local, public officials, law enforcement, faith-based communities, and non-governmental organizations following an incident of national significance related to civil rights/civil liberties. The ICCT addresses issues ranging from hate crimes reporting, reporting suspicious activities, protecting public spaces and houses of worship, and shared information on how to access additional free tools and resources available to communities. Over 355 stakeholders participated during the Orlando ICCT call. U.S. Government leaders from various agencies including DOJ's Civil Rights Division (CRT); DOJ's Community Relations Services (CRS); the FBI; the Department of Homeland Security; United States Attorneys' Offices across the country; and local and state law enforcement agencies shared with stakeholders information on protecting community centers and places of worship and how to report suspicious activities and hate crimes.

**Post-Hearing Questions for the Record
Submitted to Hon. Jeh C. Johnson
From Senator Heidi Heitkamp**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

Question#:	14
Topic:	Threats on the Northern Border
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Question: Currently, we have approximately 2,000 Border Patrol Agents trying to cover 5,500 miles of Northern Border, often in very rural parts of our nation and featuring very rough terrain. What steps need to be taken right now to mitigate threats on the Northern Border?

Response: To address and mitigate potential risks along the Northern Border, U.S. Customs and Border Protection (CBP), and specifically the U.S. Border Patrol (USBP) works in close collaboration with Canadian, federal, state, local, tribal and private industry partners to ensure timely intelligence and effective information sharing, tailored surveillance technology, and law enforcement personnel and resources with the capability to adapt and respond to the Northern Border operational environment between the ports of entry (POEs).

To combat possible threats along the Northern Border, the USBP must continue its collaborative efforts with the interagency and the public. CBP, for example, works closely with the Federal Bureau of Investigation (FBI) and the FBI's Joint Terrorism Task Forces (JTTFs). In addition, DHS must continue engaging and educating the public on the Northern Border about various issues. These communities help U.S. and Canadian law enforcement achieve enhanced situational awareness. For example, DHS established Multi-Component Intelligence Fusion Centers that facilitate the communication, intelligence and flow of information throughout a specific region to multiple law enforcement agencies.

Additionally, Northern Border Sector Intelligence Units have robust information and intelligence sharing protocols with their State, Local and Tribal and Canadian agencies through their corresponding Integrated Border Enforcement Teams and Joint Management Teams, comprised of U.S. and Canadian federal, state/provincial and local law enforcement personnel. Bi-national cooperation is further enhanced through the

Question#:	14
Topic:	Threats on the Northern Border
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

Cross Border Law Enforcement Advisory Committee (CBLEAC). The CBLEAC provides executive level guidance to cross-border law enforcement initiatives involving partnerships between United States and Canadian law enforcement agencies along our shared border. Furthermore, the USBP is establishing a Northern Border Coordination Center (NBCC) to address potential threats to the U.S./Canada border. The NBCC will serve as a central information and coordination framework that will enhance CBP's bi-national approach to actionable intelligence.

In addition, CBP in partnership with DHS Science and Technology Directorate (S&T) is developing new and improved surveillance technologies that can overcome Northern Border terrain and environmental challenges to improve targeted detection. For example, the USBP and S&T will continue collaboration with the Royal Canadian Mounted Police (RCMP) on the Canada/U.S. Sensor Sharing Pilot (CUSSP), which is intended to demonstrate the capability and operational utility of a common surveillance picture between CBP and RCMP Agents, using a combination of U.S. and Canadian sensor information. USBP also has a standing Geospatial Intelligence (GEOINT) collection requirements along 46 percent of the Northern Border, and has proposed an increase of 33 percent to include four additional USBP Sectors. USBP has been providing Capability Gap Analysis (C-GAP) training to the Royal Canadian Mounted Police (RCMP) to identify gaps along the shared border that could be exploited and to work jointly to address risks. The USBP employ regional representatives in Canada to enhance existing efforts to close and mitigate information and intelligence gaps along our shared border. Currently, there are four Border Patrol agents posted as CBP Representatives in Canada (Toronto, Vancouver, Winnipeg and Ottawa) with a fifth planned to be posted later this year for Montreal, Quebec. These USBP agents are imbedded with the Royal Canadian Mounted Police as they represent the U.S. Consulate/Embassy during engagements with Canadian agencies related to the shared border.

Additional initiatives, in varying levels of development, include the establishment of a Law Enforcement Technical Collection (LETC) Sector Intelligence Unit (SIU) program for the Northern Border; expansion of secure facilities and data network capabilities in Northern Border sectors, to allow greater exchange of classified information between DHS, CBP, and other law enforcement partners; and the expansion of maritime radar technology to enhance detection capabilities and domain awareness along the Northern Border and coastal waterways.

In addition to these efforts, the U.S. Coast Guard (USCG) and Royal Canadian Mounted Police (RCMP) collaborate under the Integrated Cross-border Maritime Law Enforcement Operations program, otherwise known as Shiprider. This program enables

Question#:	14
Topic:	Threats on the Northern Border
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

the RCMP and USCG to become designated “shipriders” who can then conduct patrols on each other’s vessels within the territorial waters of both countries. Used along with intelligence and investigative-driven operations, it provides a seamless law enforcement process that is less taxing on personnel and resources while providing more efficient and effective response to criminal activity in shared waterways. As of May 2016, there are Shiprider operations in Vancouver, BC/Blaine, WA; Windsor, ON/Detroit, MI; Kingston, ON/Alexandria Bay, NY; and Victoria, BC/Port Angeles, WA.

The United States and Canada also collaborate through integrated investigations through Border Enforcement Security Task Forces (BEST). The four Northern border BEST units incorporate personnel from Immigration and Customs Enforcement (ICE), CBP, USCG, Canada Border Services Agency (CBSA), and RCMP, as well as from other key U.S. and Canadian Federal, state, provincial, local, and tribal agencies. Through the BEST model, ICE is able to cross-designate Canadian law enforcement officers so that they receive the same authorities and protections afforded to their ICE counterparts, effectively eliminating the border as an impediment to investigations. Along the Northern border, BEST units are currently located in Blaine, Washington; Detroit, Michigan; and Buffalo and Massena, New York.

Question: How does our strategy on the Northern Border need to differ from that on the Southern Border?

Response: The operational conditions on the Northern and Southern Borders are different, both in terms of the terrain and in terms of the threats posed. DHS efforts to enhance Northern border security are guided by the goals, means, and methods outlined in the Department’s June 2012 Northern Border Strategy (NBS). The NBS is the first Department-wide strategy to guide DHS policy and operations at the U.S. Northern border. It is consistent with the Quadrennial Homeland Security Review (QHSR), the National Northern Border Counternarcotic Strategy as updated in 2014, the U.S. National Strategy for Global Supply Chain Security, and the goals of the U.S.-Canada Beyond the Border (BTB) declaration.

The NBS enables a more efficient and effective DHS presence at the Northern border by ensuring the Department’s resources are fully leveraged and efforts are not duplicated. The NBS emphasizes the use of information-sharing, personnel, technology, infrastructure, and partnerships, if appropriate, as key strategic elements necessary to achieve the three Northern border goals:

- Deter and prevent terrorism and other illegal activity;
- Safeguard and facilitate the secure flow of lawful trade and travel; and

Question#:	14
Topic:	Threats on the Northern Border
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Heidi Heitkamp
Committee:	HOMELAND SECURITY (SENATE)

- Ensure community safety and resilience before, during, and after terrorist attacks and natural disasters.

The U.S.-Canadian border presents unique security challenges due to a combination of geography, weather, and volume of trade and travel. Encompassing more than 5,500 miles (including Alaska), the Northern Border spans diverse terrain and climates, metropolitan areas and open spaces. The United States rests between two friendly nations with a long history of social, cultural and economic ties that contribute to cross-border trade and travel amounting to more than \$1 billion daily.

Our approach to the Northern Border recognizes and highlights the unique relationship between the United States and Canada.

To address and mitigate the risks presented by weather and terrain, CBP works in close collaboration with our Canadian, federal, state, local, tribal and private industry partners to ensure tailored and effective surveillance technology, law enforcement personnel, and resources are in place and have the capability to adapt and respond to the Northern border operational environment at and between POEs.

Question: When can we expect an updated threat assessment and strategy for the Northern Border?

Response: On December 15, 2016, President Obama signed the *Northern Border Security Review Act* into law, mandating that the Department of Homeland Security submit to Congress a Northern Border threat analysis by June 12, 2017. The DHS Office of Policy intends to convene a working group in January 2017 to begin the drafting process with representation from all relevant components and offices in DHS.

**Post-Hearing Questions for the Record
Submitted to Hon. Jeh C. Johnson
From Senator Joni Ernst**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

Question#:	15
Topic:	Important Federal Interest Justification
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Joni Ernst
Committee:	HOMELAND SECURITY (SENATE)

Question: To follow up on my questions asked during the hearing, I would like the following information:

When - and by whom - were ICE field offices instructed to use the "important federal interest" justification to detain individuals in the country illegally who are charged with a crime resulting in the death of an American?

Since the instruction was issued, how many times has ICE pursued removal of an illegal immigrant solely pursuant to the judgment of an ICE Field Office Director that removing that person would serve an "important federal interest"?

Response: The Department-wide civil immigration enforcement guidelines are outlined in the Department's November 2014 memorandum entitled *Policies for the Apprehension, Detention and Removal of Undocumented Immigrants*. In accordance with those guidelines, ICE may "pursue removal of an alien not identified as a priority [] provided [that], in the judgment of an ICE Field Office Director, removing such an alien would serve an important federal interest." ICE has provided guidance to its officers that removal of individuals who have been arrested for, but not yet convicted of, certain serious violent offenses may serve such an interest. This guidance was provided in March 2016. In deciding whether to pursue removal, detain or take an enforcement action in such cases, ICE considers the individual circumstances in each case. The facts of the criminal charge, as well as all other relevant factors to include immigration history and prior criminal charges, are considered by the ICE Field Office Director who makes the determination whether or not taking enforcement action in that particular case serves an important federal interest based on the totality of the circumstances.

In Fiscal Year 2016, ICE Enforcement and Removal Operations conducted 1,815 arrests of aliens whose removal was determined to serve an important federal interest.

Question#:	16
Topic:	Edwin Mejia
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Joni Ernst
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide a summary of the Department's efforts to date to apprehend Edwin Mejia.

Response: The active felony warrant for Mr. Mejia has been assigned to the U.S. Marshals Service Omaha Metro Area Fugitive Task Force. U.S. Immigration and Customs Enforcement (ICE) officers based in Omaha are assigned to assist with this case. ICE also placed Mr. Mejia on its Most Wanted List, and its National Fugitive Operations Program continues to identify and investigate leads relating to the whereabouts of Mr. Mejia.

ICE efforts to locate Mr. Mejia include the use of investigative resources from several ICE field offices in the United States and its personnel stationed abroad. ICE continues to engage with our foreign partners in Honduras for any possible leads on Mr. Mejia's current location.

Upon locating Mr. Mejia and his transfer to local law enforcement custody, ICE will work with local law enforcement to facilitate the transfer of Mr. Mejia to ICE custody at the conclusion of any criminal sentence he may be ordered to serve or upon his release from law enforcement custody.

Question#:	17
Topic:	Iraq and Syria Nonimmigrant Visas
Hearing:	Fifteen Years After 9/11: Threats to the Homeland
Primary:	The Honorable Joni Ernst
Committee:	HOMELAND SECURITY (SENATE)

Question: In Fiscal Year (FY) 2015, how many nonimmigrant visas were issued to individuals from Iraq and Syria? Of those from Iraq and Syria who were issued nonimmigrant visas in FY 2015, how many of those individuals applied for asylum at some point after entering the United States?

Response: The Department of Homeland Security does not issue either immigrant or non-immigrant visas. Therefore, we refer you to the Department of State, as the issuance of visas falls within their authority. Since the beginning of Fiscal Year 2015 until October 26, 2016, USCIS has received affirmative asylum applications from approximately 914 Syrians and 1,683 Iraqis who indicated on their asylum application as entering the United States after September 30, 2014 on a non-immigrant visa. USCIS's system for affirmative asylum applications does not track when these visas were issued. These statistics do not include defensive asylum applications.

**Post-Hearing Question for the Record
Submitted to the Honorable James Comey
From Senator Joni Ernst**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

1. In the context of discussing ISIS’s “siren song” to troubled souls everywhere during remarks last year before the National Association of Attorneys General, you stated that “those people exist in every state,” and that the FBI has “investigations of people in various stages of radicalizing in all 50 states.” Can you describe explicitly what you meant by that statement? Does that mean that ISIS is effectively present, engaged, or influencing people in varying degrees in all 50 states? Second, does the FBI continue to have homegrown violent extremist investigations in all 50 states, and what links to ISIS exist among those?

Due to the change-over in Administration, responses were never received to these questions for the record.

**Post-Hearing Questions for the Record
Submitted to Director James Comey
From Senator Tammy Baldwin**

“Fifteen Years After 9/11: Threats to the Homeland”

September 27, 2016

1. I am very concerned about self-radicalization and the increasing number of lone-wolf attacks in the United States. In your testimony, you discussed the challenge of identifying homegrown violent extremists as well as the explosion of terrorist propaganda and training that is now available online, which makes it easier for terrorists to have direct access to the United States.

I am confident that the FBI is working to counteract these threats, but I also was to ensure we are building on current techniques that are working. For example, as you know, earlier this year, the FBI prevented a terrorist attack in my home state of Wisconsin. A 23-year-old man had a vicious plan to kill at least 30 people at a Masonic Temple in downtown Milwaukee. I know that Fusion Centers and FBI databases, such as E-Guardian, were useful in preventing the attack. I also know that FBI joint terrorism task forces can be critical in sharing time-sensitive information, gathering evidence and making arrests.

How is the FBI building on these coordination tools to find the needles in the hay stack that you referenced in your testimony?

2. I am deeply concerned by the repeated attacks against various vulnerable populations in this country – the LGBT community, religious minorities, particular racial and ethnic groups – just to name a few. We held a hearing a just few months ago about the horrific tragedy in Orlando. While this was an act inspired by terrorist groups and a terrible incident of gun violence, it was also a hate crime targeting the LGBT and Latino communities. That is why I have been working to bolster federal efforts to prevent bias-motivated violence and enforce federal civil rights and hate crime laws through the Department of Justice.

What is the FBI doing to prevent hate crimes and bias-motivated attacks in its counterintelligence work?

Due to the change-over in Administration, responses were never received to these questions for the record.

**Post-Hearing Questions for the Record
Submitted to The Honorable James Comey
From Senator Heidi Heitkamp**

**“Fifteen Years After 9/11: Threats to the Homeland”
September 27, 2016**

1. There have been many recent instances of people who have a history of being aggressors in domestic disputes committing terrorist crimes. There are currently federal and state laws that require designated offenders who commit certain domestic violence offenses to be reported into the FBI’s National Instant Criminal Background Check System (NICS). Do persons who may end up on any of the multiple terror watch lists receive additional scrutiny if they have a history of domestic violence?
 - a. If so, are there concerns that given not all offenders and not all offenses are reported into the system that the FBI agents investigating certain individuals may be missing critical information?
 - b. Has the FBI studied, or otherwise analyzed, the connection between domestic violence and likelihood of committing a terrorist act among the individuals who have committed terrorist acts in the U.S. – or have otherwise been investigated as part of any terror investigations?
 - c. If so, what conclusions have you arrived at and are there ways to use this information to further prevent potential terrorist acts in the U.S.?

Due to the change-over in Administration, responses were never received to these questions for the record.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

DEC 01 2016


The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Johnson:

(U) This correspondence responds to Questions for the Record entered by Senator Baldwin (D-WI) and Senator Heitkamp (D-ND) for D/NCTC Rasmussen during the Committee's 27 September 2016 open hearing on "Fifteen Years After 9/11: Threats to the Homeland." The requested information is enclosed.

(U) If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,



Deirdre M. Walsh

Enclosure:

(U//FOUO) Response to Questions for the Record from Open Hearing on "Fifteen Years After 9/11: Threats to the Homeland."

cc: The Honorable Tammy Baldwin
The Honorable Heidi Heitkamp

Upon removal of attachment(s), this document is UNCLASSIFIED

UNCLASSIFIED FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Hearing Date: 27 September 2016
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator Baldwin
Witness: D/NCTC Rasmussen
Info Current as of: 7 November 2016
Question: 1

Question 1: (U) How does the administration assess the current desire and ability of both ISIL and al-Qa'ida to conduct external operations against the U.S. or U.S. persons and facilities abroad? Are terrorist groups moving away from more resource and time intensive external plots in favor of relying on self-radicalized, homegrown terrorists?

Answer:

(U//FOUO) We assess that the Islamic State in Iraq and the Levant (ISIL) and al-Qa'ida remain committed to attacking the Homeland and US Persons and facilities abroad based in part on these groups' past attacks, their ongoing propaganda and public statements calling for violence against the US, and the periodic arrest of group members planning new operations. These groups' varying operational agendas, capabilities, and reach will continue to shape the timing, frequency, and scope of their plots against our interests.

- a. (U//FOUO) ISIL, its branches in Africa, the Middle East, and South Asia, and its supporters worldwide probably will retain the intent and capability to launch attacks against US interests even as the group loses territory in Iraq and Syria. ISIL is pursuing a multi-pronged strategy in which it seeks to inspire its followers to conduct attacks on behalf of the group while deploying its own operatives for attacks.
- b. (U//FOUO) We assess that al-Qa'ida in the Arabian Peninsula (AQAP) is the most likely al-Qa'ida affiliate to attack the West, based on the group's history of operations in the US and Europe, including its attempted bombing of an airliner in Michigan in 2009. AQAP propaganda, including the English-language *Inspire* magazine, continues to appeal to violent extremists worldwide in its calls for lone-offender attacks against the US.
- c. (U//FOUO) We assess that the Nusrah Front, which is focused on fighting the Syrian regime, remains part of al-Qa'ida and supports its intent to target the West despite stating publicly in July that it was separating from al-Qa'ida. Al-Qa'ida leaders have relocated some of their remaining cadre from the Afghanistan-Pakistan region to Syria, where we expect that they will work with the Nusrah Front to strengthen local operations while seeking to threaten the US and its allies.

(U//FOUO) Attacks conducted in the West during the past two years do not indicate that foreign terrorist organizations (FTOs) are moving away from more resource and time intensive external plots in favor of relying on self-radicalized, homegrown terrorists. Rather, FTOs are broadening their approach to pursue a range of attacks along the spectrum of group leadership and involvement, seeking to inspire, enable, and direct attacks against the West.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Hearing Date: 27 September 2016
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator Baldwin
Witness: D/NCTC Rasmussen
Info Current as of: 7 November 2016
Question: 1 (continued)

- a. (U//FOUO) On one end of the spectrum, FTOs inspire homegrown violent extremists to conduct attacks but do not provide operational support. The perpetrators of the Orlando nightclub and San Bernardino shootings most likely were influenced by their consumption of ISIL propaganda without specific direction from the group.
- b. (U//FOUO) On the other end of the spectrum, FTOs continue to oversee the targets, timing, and tactics used against US interests. AQAP, for example, directed, executed, and publicly claimed an attempt in 2010 to mail explosives-laden cargo to the US. We also continue to see terrorist organizations, including al-Qa'ida and ISIL, directing plots against US Embassies overseas.

(U//FOUO) Along the spectrum, FTOs establish relationships with potential operatives and provide them with limited plot guidance, leaving the final attack decisions to the operatives themselves. Earlier this year, two individuals in Rhode Island were arrested and charged with conspiracy to commit acts of terrorism transcending national boundaries because they exchanged operational details online with a now-deceased ISIL member in Syria who was using social media to encourage terrorist attacks.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Hearing Date: 27 September 2016
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator Baldwin
Witness: D/NCTC Rasmussen
Info Current as of: 7 November 2016
Question: 2

Question 2: I am deeply concerned by the repeated attacks against various vulnerable populations in this country – the LGBT community, religious minorities, particular racial and ethnic groups – just to name a few. We held a hearing a just few months ago about the horrific tragedy in Orlando. While this was an act inspired by terrorist groups and a terrible incident of gun violence, it was also a hate crime targeting the LGBT and Latino communities. That is why I have been working to bolster federal efforts to prevent bias-motivated violence and enforce federal civil rights and hate crime laws through the Department of Justice. What is the NCTC doing to prevent hate crimes and bias-motivated attacks in its counterintelligence work?

Answer:

(U//FOUO) The National Counterterrorism Center (NCTC) actively works with law enforcement and local communities to raise awareness of how individuals radicalize and mobilize to violence, and helps empower local partners to enhance community resiliency. Separately, for NCTC's efforts in countering violent extremism, we defer to the Department of Justice/Federal Bureau of Investigation to discuss purely domestic terrorism related events and counter efforts.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Hearing Date: 27 September 2016
Committee: Senate Homeland Security & Governmental Affairs
Member: Senator Heitkamp
Witness: D/NCTC Rasmussen
Info Current as of: 7 November 2016
Question: 1

Question 1: (U) In August of 2016, President Obama cited key military victories against ISIL and stated that ISIL was "inevitably going to be defeated." Is the progress that our military is making against ISIL having an effect on their ability to recruit? Are we successfully countering the narrative that ISIL is propagating/spreading online?

Answer:

(U) The flow of foreign fighters to Syria and Iraq has decreased. Additionally, as provided in Director Rasmussen's Statement for the Record, "ISIL has lost over half its territory in Iraq and nearly a quarter in Syria; the number of fighters it has in those countries is significantly down, and its illicit income streams are down. But despite this progress, it is our judgment that ISIL's ability to carry out terrorist attacks in Syria, Iraq, and abroad has not to date been significantly diminished, and the tempo of ISIL-linked terrorist activity is a reminder of the group's continued global reach." Director Rasmussen further stated that: "While ISIL's efforts on the ground in Syria and Iraq remain a top priority for the group's leadership, we do not judge that there is a direct link between the group's current battlefield status in Iraq and Syria and the group's capacity to operate as a terrorist organization with global capabilities. Their external operations capability has been building and entrenching during the past two years, and we do not think battlefield losses alone will be sufficient to completely degrade the group's terrorism capabilities."

(U//FOUO) We believe that progress has been made in countering ISIL's online propaganda campaign. For example, in the second quarter of 2016, ISIL released 1,725 official media products, a 7-percent decrease from the group's production levels in the first quarter, according to NCTC and Open Source Enterprise analysis of ISIL media releases on Twitter. This is the third consecutive quarter in which ISIL's media output has declined from its peak of 2,281 products in the third quarter of 2015, a drop of almost 25 percent. We expect to see a continued decline in the third quarter of 2016, because of ongoing setbacks to the group.

- a. We continue to assess that ISIL's battlefield defeats in Iraq and Syria and loss or reassignment of media personnel have driven the decrease, according to open sources.
- b. In the past year, the amount of pro-ISIL Twitter content has declined significantly, according to a press report.
- c. In September 2015, Twitter began increasing suspensions of ISIL-linked accounts that violated the company's terms of service and, as of August 2016, publicly claimed to have taken down at least 360,000 handles related to ISIL.

UNCLASSIFIED//FOR OFFICIAL USE ONLY