WORLDWIDE THREATS TO THE HOMELAND: ISIS AND THE NEW WAVE OF TERROR

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 14, 2016

Serial No. 114–83

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

25–265 PDF WASHINGTON : 2017

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

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

CONTENTS

WORLDWIDE THREATS TO THE HOMELAND: ISIS AND THE NEW WAVE OF TERROR

Thursday, July 14, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:06 a.m., in room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the committee] presiding.

Present: Representatives McCaul, Smith, King, Rogers, Duncan, Marino, Barletta, Perry, Katko, Hurd, Carter, Walker, McSally, Ratcliffe, Donovan, Thompson, Sanchez, Jackson Lee, Langevin, Keating, Payne, Vela, Watson Coleman, and Torres.

Chairman MCCAUL. The Committee on Homeland Security will come to order. The purpose of this hearing is to receive testimony regarding threats to our homeland around the globe.

Before I begin my opening statement, I would like to take a moment to remember the Dallas police officers who lost their lives in the line of duty last week.

[Moment of silence.]

Chairman MCCAUL. We will never forget. The tragedy reminds us that every day our first responders take risks to protect us, and we can honor their sacrifice by showing that we support them and that we have their backs.

In the past month, we witnessed 4 major terrorist attacks in 4 weeks in 4 countries, including the deadliest terrorist attack on the United States homeland since 9/11. All these attacks are believed to be the work of ISIS, the new standard-bearer of evil. In fact, the group has now been linked to almost 100 plots against the West since 2014, an unprecedented wave of terror.

Nearly 15 years after 9/11, we must confront the reality that we are not winning the war against Islamist terror. While groups like ISIS may be losing some ground in Syria and Iraq, overall, they are not on the run; they are on the rise. I am concerned that we have only seen the tip of the iceberg.

Director Comey, you prophetically warned this committee 2 years ago that there would eventually be a terrorist diaspora out of Syria and Iraq, with jihadists returning home to spread extremism. That exodus has now begun. Thousands of Western foreign fighters have departed the conflict zone, including operatives who are being sent to conduct attacks, as we saw in Paris and in Brussels. At the same time, ISIS's on-line recruiting has evolved, and they now micro-target followers by language and country.

Although our Nation is shielded by two oceans, geography alone cannot protect us from this mortal threat. The statistics speak for themselves. In the past 2 years, Federal authorities have arrested more than 90 ISIS supporters in the United States, and in 2015, we saw more home-grown jihadist plots than we have ever tracked in a single year. I commend your agencies for stopping dozens of potential tragedies, but too many have already slipped through the cracks, and we know that more plots are in the pipeline.

In the wake of Orlando, Americans are demanding to know how we got to this point, and a clear majority of them say Washington is not doing enough to roll back this threat. They are stunned by the political correctness here in our Nation's capital, especially the refusal to call the threat what it is. We must define the threat in order to defeat it, just as we did with communism and fascism. We cannot hide the truth, and we cannot redact it from reality.

So let's be frank about who the enemy is. We are fighting radical Islamists. These fanatics have perverted a major religion into a license to kill and brutalize, and while their beliefs do not represent the views of the majority of Muslims, they represent a dangerous global movement bent on conquering and subjugating others under their oppressive rule.

Sadly, we have failed to commit the resources needed to win. I was recently on the USS TRUMAN aircraft carrier in the Persian Gulf, where our sailors are launching sorties to destroy ISIS positions. While I am proud of their efforts, I am not encouraged by our progress.

Last month, CIA Director John Brennan gave the administration a failing grade in the fight and said that, "Our efforts have not reduced the groups' terrorism, capability, and global reach."

The President is sticking to a strategy that is better suited for losing a war than winning one. Each day we stick with half measures, ISIS is able to dig in further and advance a murderous agenda across the globe—another day to plot and another day to kill.

The violence is becoming so frequent that we now simply refer to jihadist attacks by the name of the city in which they were perpetrated: Paris, Chattanooga, San Bernardino, Brussels, Orlando, Istanbul. How many more will be added to the list before we get serious about taking the fight to the enemy?

This is the greatest threat of our time, and I urge each of you here today to explain to this committee and to the American people how you are planning to elevate our defenses to keep Americans safe.

With that, the Chair now recognizes the Ranking Member, Mr. Thompson.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

JULY 14, 2016

Before I begin today's hearing I would like to take a moment to remember the Dallas police officers who lost their lives in the line of duty last week. We will never forget.

The tragedy reminds us that every day our first responders take risks to protect us, and we can honor their sacrifice by showing that we support them and that we have their backs.

The past month we witnessed 4 major terrorist attacks, in 4 weeks, in 4 countries, including the deadliest terrorist attack on the United States homeland since 9/11.

All of these attacks are believed to be the work of ISIS, the new standard-bearer of evil. In fact, the group has now been linked to almost 100 plots against the West since 2014—an unprecedented wave of terror.

Nearly 15 years after 9/11, we must confront the reality that we are not winning the war against Islamist terror.

While groups like ISIS may be losing some ground in Syria and Iraq, overall they are not "on the run," as the Obama administration says. They are on the rise.

But I am concerned that we have only seen the tip of the iceberg.

Director Comey, you prophetically warned this committee 2 years ago that there would eventually be a "terrorist diaspora" out of Syria and Iraq, with jihadists returning home to spread extremism.

The exodus has now begun. Thousands of Western foreign fighters have departed the conflict zone, including operatives who are being sent to conduct attacks, as we saw in Paris and Brussels. At the same time, ISIS' on-line recruiting has evolved, and they now micro-target followers by language and country.

Although our Nation is shielded by two oceans, geography alone cannot protect us from this mortal threat.

The statistics speak for themselves. In the past 2 years, Federal authorities have arrested more than 90 ISIS supporters here in our country, and in 2015 we saw more home-grown jihadist plots than we have ever tracked in a single year.

I commend your agencies for stopping dozens of potential tragedies, but too many have already slipped through the cracks. We know that more plots are in the pipeline.

In the wake of Orlando, Americans are demanding to know how we got to this point, and a clear majority of them say Washington is not doing enough to roll back the threat.

They are stunned by the political correctness here in our Nation's capital, especially the refusal to call the threat what it is. We must define the threat in order to defeat it—just as we did with communism and fascism.

We cannot hide the truth, and we cannot redact it from reality. So let's be frank about the enemy: We are fighting radical Islamists.

These fanatics have perverted a major religion into a license to kill and brutalize. And while their beliefs do not represent the views of a majority of Muslims, they represent a dangerous global movement bent on conquering and subjugating others under their oppressive rule.

Sadly, we have failed to commit the resources needed to win. I was recently on the USS Truman aircraft carrier in the Persian Gulf, where our sailors are launching sorties to destroy ISIS positions. While I am proud of their efforts, I am not encouraged by our progress.

Last month, even CIA Director John Brennan gave the administration a failing grade in the fight and said that, "our efforts have not reduced the group's terrorism capability and global reach."

The President is sticking to a "drip, drip" strategy that is better suited for losing a war than winning one. And each day we stick with half-measures, ISIS is able to dig in further and advance a murderous agenda across the globe. Another day to plot, another day to kill.

The violence is becoming so frequent that we now simply refer to jihadist attacks by the name of the city in which they were perpetrated: Paris. Chattanooga. San Bernardino. Brussels. Orlando. Istanbul.

How many more will be added to the list before we get serious about taking the fight to the enemy?

This is the greatest threat of our time, and I urge each of you today to explain to this committee—and to the American people—how you are planning to elevate our defenses to keep Americans safe.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Before I begin, I want to express also my condolences to the families affected by violence in recent weeks. Today, the pain that is felt by families in Baton Rouge, Dallas, Falcon Heights, and Orlando is reverberating across the country.

I want to thank Director Comey and Director Rasmussen for their service and for appearing before us today.

Secretary Johnson, I also want to thank you for your service. This is likely your last time that you will testify in this room, the

very room where your grandfather testified in 1949. When Joe McCarthy called your grandfather to testify 67 years ago, it was a time of heated, divisive rhetoric and fear, fear of infiltration by the Communist ideology. Unfortunately, today, the Nation finds itself again in a period of heated rhetoric fueled by fear.

Today, Americans legitimately fear infiltration by the violent ideology espoused by ISIL. Last month's horrific terrorist attack in Orlando, Florida, underscores ISIL's violent ideology in reaching Americans and inspiring terrorism. Without training, direction, or support by a foreign terrorist organization, the Orlando assailant, armed with an AR-type rifle and 9-millimeter semiautomatic pistol, carried out the deadliest shooting in American history. During the attack, the shooter pledged allegiance to ISIL, but prior to the attack, he historically aligned himself with competing foreign terrorist organizations. Soon after, evidence emerged that the shooter may have been motivated by racism and homophobia. Yet, in the hours and days post-Orlando, members of this body and the Executive branch wasted no time labeling this tragedy as an act of terrorism.

In contrast, last summer, when a gunman, who, like the Orlando shooter, was radicalized on-line, opened fire on 9 parishioners in a Charleston, South Carolina, church, many in this body and, indeed, the Executive branch refused to label this attack an act of terrorism.

Last week, a gunman, who we understand through his on-line activities subscribed to a violent political ideology that runs counter to American values, ambushed police officers in Dallas, Texas, at a peaceful protest to send a political message, yet many of the same people in this body and the administration who labeled past mass shootings that were inspired by a foreign terrorist organization as an act of terrorism were quick to dismiss the notion that the Dallas attack was an act of terrorism.

While foreign terrorist organizations like ISIL represent a significant homeland security threat, today's threat environment is far more diverse than back in 1949, when this room was used to investigate the threat posed by one ideology, communism.

Those who single-mindedly focus on one ideology or group, namely ISIL, run the risk of leaving us vulnerable to attacks by other foreign terrorist organizations, like al-Qaeda, and even domestic terrorist organizations.

To underscore the domestic terrorism threat, I note that earlier this year, anti-Government extremists took over a Federal facility in Oregon, threatening the security of Federal Government employees for 41 days. Law enforcement officers consistently ranked the threat from anti-Government groups higher than the threat from foreign terrorist organizations. Still, the same voices that were so quick to label incidents in Orlando and San Bernardino acts of terrorism have largely been silent about the heightened threat environment associated with anti-Government groups.

Today's witnesses, you may be chided by my Republican colleagues for the fact that, in your written testimony, the phrase "radical Islamist terrorism" is not used. However, fixation on that phrase is misplaced insofar as the threat posed by ISIL and other foreign terrorist organizations receives significant attention in the

testimony. More troubling is the fact that nowhere in your testimony is there a passing mention of domestic terrorism or anti-Government groups. Terrorist-inspired lone-wolf or small-scale attacks can be inspired by foreign or domestic actors.

To respond to this new wave of terror, inspired mainly by propaganda on the internet, the administration is pursuing programs to counter violent extremism. Putting aside the fact that there is some debate on the effectiveness of such programs, I have questions about whether the agency charged to carry out the administration's CVE efforts are working to prevent terrorist recruitment and radicalization by all types of terrorist groups. I was happy to learn from the Secretary this morning that they just this week pushed out the directives for the $10 million allocation for the CVE grant funding.

Beyond the discussion of CVE, however, I look forward to engaging the witnesses in an issue common to the attacks in Orlando, San Bernardino, Charleston, and Dallas: The availability of assault weapons to terrorists. We must be able to keep guns out of the hands of terrorists. Members of Congress, the administration, and the American public recognize this. However, Speaker Ryan and Republican leadership continue to approve empty gestures posing as legislation instead of bringing up a vote on sensible gun control. We know that the common thread between most recent attacks, both inspired by foreign and domestic actors on American soil, has two commonalities: Radicalization and assault weapons. I do not accept the notion that nothing can be done to address the availability of military-style firearms to individuals who intend to do harm to our country. When it comes to protecting this Nation, Congress will be rightfully judged by the American people on whether it tackles both.

Thank you, Mr. Chair. I yield back and look forward to the testimony.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 14, 2016

Unfortunately, today, the Nation finds itself in a period of heated rhetoric-fueled by fear. Today, Americans legitimately fear infiltration by the violent ideology espoused by ISIL. Last month's horrific terrorist attack in Orlando, Florida, underscores that ISIL's violent ideology is reaching Americans and inspiring terrorism.

Without training, direction, or support by a foreign terrorist organization, the Orlando assailant, armed with an AR-type rifle and 9mm semi-automatic pistol, carried out the deadliest shooting in American history.

During the attack, the shooter pledged allegiance to ISIL but prior to the attack, he historically aligned himself with competing foreign terrorist organizations. Soon after, evidence emerged that the shooter may have also been motivated by racism and homophobia. Yet, in the hours and days post-Orlando, Members of this body and the Executive branch wasted no time labeling this tragedy as an "act of terrorism."

In contrast, last summer, when a gunman, who, like the Orlando shooter was radicalized on-line, opened fire on 9 parishioners in a Charleston, South Carolina, many in this body and, indeed, the Executive branch, refused to label this attack an "act of terrorism."

Last week, a gunman who we understand, through his on-line activities, ascribed to a violent political ideology that runs counter to American values, ambushed police officers in Dallas, Texas, at a peaceful protest to send a political message.

Yet, many of the same people in this body and the administration who labeled past mass shootings that were inspired by foreign terrorist organizations as "acts

of terrorism," were quick to dismiss the notion that the Dallas attack was an act of terrorism.

While foreign terrorist organizations like ISIL represent a significant homeland security threat, today's threat environment is far more diverse than back in 1949, when this room was used to investigate the threat posed by one ideology—communism.

Those who single-mindedly focus on one ideology or group—namely "ISIL"—run the risk of leaving us vulnerable to attacks by other foreign terrorist organizations like al-Qaeda and even by domestic terrorist groups.

To underscore the domestic terrorism threat, I would note that earlier this year, anti-Government extremists took over a Federal facility in Oregon, threatening the security of Federal Government employees for 41 days. Law enforcement officers consistently rank the threat from anti-Government groups higher than the threat from foreign terrorist organizations.

Still, the same voices that were so quick to label incidents in Orlando and San Bernardino "acts of terrorism" have largely been silent about the heightened threat environment associated with anti-Government groups.

To today's witnesses, you may be chided by my Republican colleagues for the fact that, in your written testimony the phrase "radical Islamist terrorism" is not used. However, fixation on that phrase is misplaced, insofar as the threat posed by ISIL and other foreign terrorist organizations receives significant attention in the testimony.

More troubling, is the fact that nowhere in your testimonies is there even a passing mention of domestic terrorism or anti-Government groups. Terrorist-inspired lone-wolf or small-cell attacks can be inspired by foreign and domestic actors.

To respond to this new wave of terror, inspired mainly by propaganda on the internet, the administration is pursuing programs to counter violent extremism. Putting aside the fact that there is some debate on the effectiveness of such programs, I have questions about whether the agencies charged to carry out the administration's CVE efforts are working to prevent terrorist recruitment and radicalization by all types of terrorist groups.

I am troubled that the Department of Homeland Security recently announced $10 million in CVE grant funding but has yet to issue the Department-wide strategy which I have been requesting for over a year and have consistently been told is "forthcoming."

Beyond the discussion of CVE, I look forward to engaging the witnesses on an issue common to the attacks in Orlando, San Bernardino, Charleston, and Dallas—the availability of assault weapons to terrorists.

We must be able to keep guns out of the hands of terrorists. Members of Congress, the administration, and the American public recognize this. However, Speaker Ryan and Republican leadership continue to approve empty gestures posing as legislation instead of bringing up a vote on sensible gun control.

We know that the common thread between the most recent attacks—both inspired by foreign and domestic actors—on American soil had two commonalities: Radicalization and assault weapons. I do not accept the notion that nothing can be done to address the availability of military-style firearms to individuals with intent to do harm to our country. When it comes to protecting this Nation, Congress will be rightfully judged by the American people on whether it tackles both.

Chairman MCCAUL. I thank the Ranking Member.

Other Members are reminded that opening statements may be submitted for the record.

[The statement of Hon. Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

JULY 14, 2016

Chairman McCaul, Ranking Member Thompson, thank you for this opportunity to hear testimony on "Worldwide Threats to the Homeland: ISIS and the New Wave of Terror."

Today's hearing is an opportunity for the committee to receive testimony from the witnesses about terrorist threats, including the radicalization and terrorism recruitment in the United States and abroad.

We will also receive testimony about what the Executive branch is doing to counter both home-grown and domestic violent extremism.

I join my colleagues on the committee in welcoming the Secretary of Homeland Security Jeh Johnson, FBI Director James Corney, and Nick Rasmussen, director of the National Counterterrorism Center to today's hearing.

As a senior Member of the House Committee on Homeland Security and Ranking Member of the Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations the topic of threats to homeland security is of significance and especially in light of recent events.

My primary domestic security concerns are:

- preventing foreign fighters and foreign-trained fighters from entering the United States undetected;
- countering international and home-grown violent extremism;
- addressing the uncontrolled proliferation of long-guns that are designed for battlefields and not hunting ranges;
- controlling access to firearms for those who are deemed to be too dangerous to fly;
- Protecting critical infrastructure from physical and cyber attack; and
- Strengthening the capacity of the Department of Homeland Security and the Department of Justice to meet the challenges posed by weapons of mass destruction.

FOREIGN FIGHTERS AND FOREIGN-TRAINED FIGHTERS

I initially introduced the "No Fly for Foreign Fighters Act" after the investigation of an attempt to detonate explosives on a Northwest Airlines Flight on Christmas day 2009.

Investigation of the incident revealed that counterterrorism agencies had information that raised red flags about this individual, referred to as the "underwear bomber," but the dots were not connected and he was not placed in the Terrorist Screening Data base or the TSDB.

This incident shone a spotlight on potential gaps in our watch list programs, and terrorists screening process, which indicate significant improvements were needed. That said, questions about the system remain.

In fact, it is not uncommon to see news of a flight being diverted or an emergency landing because a passenger happened to be on the No-Fly list but there was a delay getting that information.

It is even more common to read articles about the frequency of false positives and individuals being mistakenly identified as being on the list—causing them and their fellow passenger significant delay and frustration.

The issue of false positives is something that I know many of my colleagues on the committee are particularly interested in, as well as groups such as the ACLU.

In light of the events of the last 12 months, however, the issue of homeland security and, in particular, the accuracy of our screening and watchlisting process has become even more significant to me.

More than 30,000 foreign fighters from at least 100 different countries have traveled to Syria and Iraq to fight for ISIL since 2011.

In the last 18 months, the number of foreign fighters traveling to Syria and Iraq has more than doubled.

In the first 6 months of 2015, more than 7,000 foreign fighters have arrived in Syria and Iraq.

Of those traveling to Syria and Iraq to fight for the Islamic State terrorist group, it is estimated at least 250 hold U.S. citizenship.

The accuracy of our terrorist screening tools are more critical now than ever before.

That is why I worked with the Chairman of the Judiciary Committee and Mr. Ratcliffe who is a Member of the Judiciary Committee and Homeland Security, to introduce H.R. 4240, which mandates an independent review of the TSDB's operation and administration.

Although the inspector general for the Department of Justice conducts annual audits of the TSDB, there has not been an independent review since the GAO study after the 2009 incident.

H.R. 4240 directs the GAO to conduct an independent review of the operation and administration of the TSDB, and subsets of the TSDB, to assess: (1) Whether past weaknesses have been address; and (2) the extent to which existing vulnerabilities may be resolved or mitigated through additional changes.

The legislation was drafted broadly, to allow the GAO to conduct a comprehensive review not just of the TSDB's accuracy, but of its entire operation and administration.

Following its study, the GAO will submit a report to the House and Senate Judiciary Committees, with its findings and any recommendations for improvements.

H.R. 4240, which passed the House under suspension, is the next step in ensuring that the screening and watchlisting process works as it is intended.

COUNTERING VIOLENT EXTREMISM AT HOME AND ABROAD

One of the enduring challenges for Members of this committee is how we guide the work of the Department of Homeland Security.

One challenge we have faced is finding definitions for terrorism that will address the reality that these acts are intended to intimidate or terrorize the public or a minority group.

Understanding what terrorism is begins in law with its definition.

Title 22 of the U.S. Code, Section 26S6f(d) defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."

The FBI defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

Terrorism is a violation of the criminal laws of the United States or of any State or other subdivision of the United States and appears to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

DHS defines Domestic Terrorism as:

"Any act of violence that is dangerous to human life or potentially destructive of critical infrastructure or key resources committed by a group or individual based and operating entirely within the United States or its territories without direction or inspiration from a foreign terrorist group."

Groups and individuals inspired to commit terrorist acts are motivated by a range of personal, religious, political, or other ideological beliefs—there is no magic formula for determining the source of terrorism.

Further, the complexity of adding social media as a new source of recruitment for violent extremists is complicating the efforts of law enforcement, domestic security, and National defense.

The line between lawfully-protected speech and activity that may be to some radical—should be clearly defined.

Taking care to protect civil liberties and Constitutional rights means that our system of laws must acknowledge that reading, writing, or speaking one's views or beliefs even when they are unpopular is not a crime.

Hate speech is not a crime—while an act of violence motivated by hate is a crime.

Violent Extremist threats within the United States can come from a range of violent extremist groups and individuals, including Domestic Terrorists and Homegrown Violent Extremists (HVEs).

In the wake of the killings at Mother Emanuel in Charlotte South Carolina; San Bernardino; the Pulse Night Club in Orlando; and the murder of 5 police offers protecting participants in a peaceful demonstration in Dallas, Texas it is evident that home-grown violent extremism is a threat that must be addressed.

REDUCTION IN WEAPONS OF WAR ON U.S. STREETS AND EASE OF ACCESS TO GUNS FOR THOSE ON THE NO-FLY LIST

Gun violence carnage that claimed the lives of more than 300,000 persons during the period 2005–2015, include the following:

1. On July 7, 2016, in Dallas Texas 4 police officers and 1 transit officer were killed by a lone gun man using a AK–74 assault-style rifle and a handgun;
2. On June 12, 2016, in Orlando, Florida at the Pulse nightclub a single shooter armed with a .223 caliber AR type rifle and 9mm semiautomatic pistol killed 49 people and left 53 injured;
3. On December 2, 2015 in San Bernardino, California, two gunmen armed with two .223 caliber AR–15-type semi-automatic rifles and two 9mm semi-automatic pistols killed 14 people and injured 21 others at the Inland Regional Center;
4. On July 7, 2015 in Chattanooga, Tennessee a gunman shot and killed 5 people, including 2 U.S. Marines and a Naval Officer, and shot and injured 2 others at a recruiting center and U.S. Naval Reserve Center;
5. On June 7, 2015, a gunman shot and killed 9 people at the Mother Emanuel African Methodist Episcopal Church in Charleston, South Carolina, one of the oldest and largest black congregations in the South;

6. On August 5, 2012 in Oak Creek, Wisconsin, a gunman shot and killed 6 people, and injured 3 others, at the Sikh Temple of Oak Creek;

7. On December 14, 2012, a gunman using a Bushmaster .223 caliber model XM15 rifle with a 30 round magazine in 5 minutes murdered 26 persons, including 20 children and 6 school administrators and teachers, at Sandy Hook Elementary in Newtown, Connecticut;

8. On November 11, 2009, at Fort Hood, near Killeen, Texas, a gunman shot and killed 13 people, and wounded 30 others; and

Nearly 100 metropolitan areas have experienced mass shootings like these since 2013.

Mass shootings occur more frequently in States that do not require background checks for all gun sales, and analyses of mass shootings in the United States between 2009 and 2015 document that the majority of mass shootings occur in venues where the carrying of firearm is not restricted.

I have introduced two measures that specifically address issues of gun safety raised by the carnage over the last few years.

The first bill is H.R. 3125 "Accidental Firearms Transfers Reporting Act of 2015," which seeks to shed light on the gun purchase loophole that led to Dylan Roofs tragic possession of the firearm used to murder 9 innocent persons at Emanuel A.M.E. Church in Charleston, South Carolina, as well as the numerous other cases where a firearm was handed over to an unintended and potentially dangerous recipient.

The bill would require the director of the Federal Bureau of Investigations to report to Congress the number of firearm transfers resulting from the failure to complete a background check within 3 business days.

The FBI is further instructed to disclose and report on the procedures in place and actions taken after discovering a firearm has been transferred to a transferee who is ineligible to receive a firearm.

This bill directs the FBI to report on the erroneous transfer of firearms every 6 months to ensure internal oversight and effective monitoring to expose any other patterns or practices in need of administrative or legislative action.

I have also introduced, H.R. 5470, "Stopping Mass Killings By Violent Terrorists Act," gives our law enforcement agencies another tool to help keep the most dangerous weapons out of the hands of home-grown terrorists.

H.R. 5470, the "Stopping Mass Killings by Violent Terrorists Act," prohibit a firearms dealer from transferring a semiautomatic assault weapon or large-capacity ammunition clips to a purchaser until the Attorney General has verified that the prospective transferee has truthfully answered new questions on the firearms background check questionnaire regarding contacts between the prospective purchaser or transferee and Federal law enforcement authorities.

Specifically, H.R. 5470 requires and provides that:

(1) with respect to any firearm or large-capacity ammunition feeding device, the attorney general update the Background Check Questionnaire to include questions relating to the existence and nature of any contacts with Federal law enforcement agencies within the prior 24 months;
(2) for a purchaser questionnaire, affirming the existence of contacts with Federal law enforcement agencies, that the purchase of a covered firearm cannot be consummated until affirmative approval is received by the FBI; and
(3) with respect to any firearm or large-capacity ammunition feeding device (LCAFD), any purchaser who refuses or fails to provide the information required, the Transferor (Seller) shall nevertheless submit the uncompleted questionnaire to the FBI for further review or investigation.

On average gun violence claims the lives of 90 persons each day. Since 1968, more than a million persons have died at the hand of a gun. The homicide rate in the United States is about 6.9 times higher than the combined rate in 22 other highly-developed and populous countries, despite similar non-lethal crime and violence rates.

SECURING CRITICAL INFRASTRUCTURE

Last year Assistant Secretary Caitlin Durkovich informed a gathering of energy firm executives at an energy conference that ISIS has been attempting to hack American electrical power companies.

Critical infrastructure is dispersed throughout the United States and if primarily under the control of private owners or non-government operators; and includes:

- The Electronic Utility Grid;
- Water Treatment facilities;
- Ports, railways, and highways;

- Telecommunication System;
- Food production, processing, and distribution;
- Health care delivery system; and

FINANCIAL SYSTEM

Critical infrastructure relies upon distributed computer networks to support vital functions and delivery systems.

The security of computing networks rely upon strong encryption and protocols to assure that the security of encryption passwords and network access is maintained.

To support the work of the Department of Homeland Security in providing cyber protection to critical infrastructure, I introduced H.R. 85, the Terrorism Prevention and Critical Infrastructure Protection Act.

The bill facilitates research and development activities to strengthen the security and resilience of the Nation's critical infrastructure against terrorist attacks and All-Hazard events.

The bill establishes research initiatives that would provide the Secretary of Homeland Security with a report on:

- the degree that certain critical infrastructure is reliant upon other types of critical infrastructure;
- programs that would improve professional development for security professionals;
- assessment of vulnerabilities in software systems, firewalls, applications, and methods of analyzing cybersecurity; and
- coordination of Federal agencies' response to cyber terrorism incidents.

The bill would take an in-depth approach to securing critical infrastructure.

H.R. 85 would provide oversight committees and Members of Congress with a better understanding of the terrorism preparedness of critical infrastructure owners and operators, contractors, or non-Government agency entities that provide computer-related support or services to critical infrastructure.

DHS Protective Security Coordination Division (PSCD) is established to conduct specialized field assessments to identify vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on the Nation's critical infrastructure.

I am particularly interested in the work of the DHS PSCD office because of a Jackson Lee amendment adopted last year under House consideration of the H.R. 1731, "National Cybersecurity Protection Advancement Act of 2015."

The Jackson Lee amendment allowed the Secretary of Homeland Security to consult with sector-specific agencies, businesses, and stakeholders to produce and submit to the Committee on Homeland Security a report on how best to align Federally-funded cybersecurity research and development activities with private-sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure.

The amendment included a cybersecurity research and development objective to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology.

Finally, this Jackson Lee Amendment supports investigation into enhanced computer-aided modeling capabilities to determine potential impacts on critical infrastructure of incidents or threat scenarios, and cascading effects on other sectors; and facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen cybersecurity and resilience.

CYBERSECURITY CHALLENGES

The arrival of the Internet of Things, which will introduce ubiquitous wireless technology far beyond the limitations of computers or computing devices to include practically every physical object in our environment.

The cybersecurity challenges of tomorrow will look very different from the cybersecurity challenges of today.

One of the chief concerns of the FBI is the use of encryption by criminals and terrorist to hide information on the internet.

This is not a new concern, the use of techniques that facilitate Government access to encryption products was litigated by the Justice Department during the Clinton administration in 1990s at the time the general public began using the internet.

Computing technologists, cybersecurity experts, companies, civil liberties organizations, researchers, and innovators strongly oppose this approach then as they do today.

One of the major problems with trying to control who has access to strong encryption is how easy it is to get or create an encryption computer program.

In the research I had my staff conduct, it was easy to find encryption programs on the internet that were written by academics, researchers, students, and others with the requisite level of computing programming knowledge.

In fact, I found that keeping an algorithm secret, for the purpose of security, is universally considered as a sign that the encryption program is likely poorly written.

In my analysis of the facts regarding this very complex area of computing security the most important knowledge to possess is the password or key.

The other important cybersecurity component is well-trained personnel who must do the work in protecting computing systems and information assets.

WEAPONS OF MASS DESTRUCTION

In the not-too-distant future, the harnessing of nuclear energy will no longer be the privilege of only a few nations.

Today, nuclear energy is under serious consideration in more than 55 developed and developing countries and an additional 60 countries are expressing interest in, considering, or actively planning for nuclear power.

These efforts, if successful, would represent a quadrupling of today's 30 nuclear powered nations.

These ambitious nations face immense security challenges and for these reasons the United States should be working to develop relationships with nations who are willing to accept our assistance in developing peaceful nuclear programs.

However, I believe that we should take this effort one step further by developing the infrastructure to move excess nuclear material and waste from these nations so that it may be safely disposed of without concern that it could fall into unfriendly hands.

I will soon introduce legislation to establish much-needed foresight in meeting the future challenges posed by the emergency of nuclear power in developing nations.

In my statement I have outlined several areas of particular concern regarding Worldwide Threats and Homeland Security Challenges.

I thank today's witnesses for their testimony and look forward to the opportunity to ask questions.

Thank you.

Chairman MCCAUL. We are pleased to have a distinguished panel of witnesses before us today on this important topic. First, the Honorable Jeh Johnson, Secretary of the Department of Homeland Security. I believe this possibly could be your last testimony before this committee, and we appreciate your service to the Nation.

Next, the Honorable James Comey, director of the FBI at the U.S. Department of Justice, and then, finally, the Honorable Nicholas Rasmussen, director of the National Counterterrorism Center in the Office of the Director of National Intelligence.

I thank all of you for being here today. The Chair now recognizes Secretary Johnson to testify.

STATEMENT OF HONORABLE JEH C. JOHNSON, SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Secretary JOHNSON. Thank you, Mr. Chairman, Congressman Thompson, Members of this committee. You have my prepared statement for the record. I will just offer a few remarks here briefly.

I want to thank this committee for the productivity in cranking out legislation that I believe has indeed helped secure our homeland in the time that I have been Secretary. I have observed this committee work in a collaborative fashion, and it has been really productive, so I thank you for that.

I want to thank my colleagues, Nick and Jim, for our work together protecting the homeland.

Lots of people ask me what keeps me up at night. It is hard to prioritize and rank what keeps me up at night. I have a lot of things that keep me up at night, but if you ask me to rank them, my best effort I would have to say the prospect of home-grown violent extremism—another San Bernardino, another Orlando—is No. 1 on my list. We deal in this age not just with the terrorist-directed attack but the terrorist-inspired attack and now a new category of terrorist-enabled attacks. These are things that keep me up at night. It is difficult for our law enforcement and our intelligence community to detect the self-radicalized actor.

Foreign terrorist travel, the prospect of foreign terrorist travel to our homeland keeps me up at night. Of course, cybersecurity, aviation security, border security, the prospect of what we refer to as special interest aliens arriving on our Southern Border are things that we should all be focused on and dedicated to addressing.

Militarily, we continue to take the fight, pursuant to the President's strategy, to the Islamic State and al-Qaeda overseas. I have been pleased with the number of strikes that have taken out leaders of the Islamic State, particularly those focused on external attacks. Of course, our intelligence community and law enforcement efforts to protect the homeland here continue.

I have a lot of confidence in the FBI, under Jim's leadership in particular, with their aggressive counterterrorism law enforcement efforts. We together have worked much more actively in the last 2 years, I think, with State and local law enforcement on protecting the homeland and sharing information about what we see on a National and international level. Active-shooter training for local law enforcement is something that, since I have been Secretary, we have prioritized and enhanced through our National Targeting Center at Customs and Border Protection, and with better data collection and sharing of data, I think we do a better job of knowing who is traveling to the United States and knowing about individuals of suspicion before they get here to put them on a watch list, a selectee list, and what have you.

We have enhanced the security around our Visa Waiver Program. With the help of this Congress last year, we now have the ability to deny visa-free travel to those who have traveled to Syria, Sudan, Iraq, Iran, and, as a result of the three new countries I added to the list because of this new legislative authority, Yemen, Somalia, and Libya.

Public vigilance and public awareness must be keys to our efforts in combating home-grown violent extremism. Public awareness, public vigilance can and do make a difference.

Along with our CVE efforts that Congressman Thompson focused on, I am pleased that there appears to be bipartisan support for continued efforts at countering violent extremism. I am pleased that we have grant money this year to combat it. I hope that, in future years, Congress will provide us with more grant money.

I look forward to questions from this committee in terms of our aviation security efforts, efforts to secure the Republican and Democratic National Conventions. I personally plan to travel to Cleveland tomorrow and to Philadelphia next week to inspect the security at both convention sites.

In general, we encourage the public to continue to travel, to continue to associate, to celebrate the holidays, celebrate the summer season, but public vigilance and public awareness can and do make a difference in this current environment.

Thank you. I look forward to your questions.

[The prepared statement of Secretary Johnson follows:]

PREPARED STATEMENT OF HON. JEH C. JOHNSON

JULY 14, 2016

Chairman McCaul, Representative Thompson, 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 the homeland is important. I welcome the opportunity to be here again.

COUNTERTERRORISM

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. By their nature, terrorist-inspired attacks are often 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.

This threat environment has required a whole new type of response.

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 47% 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 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.

And, 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 helped to fund an active-shooter training exercise that took place in the New York City subways last November, a series of these exercises earlier this year in Miami and Louisville, and just last month at Fenway Park in Boston. In February, and last month, we announced another two

rounds of awards for fiscal year 2016 that will fund similar activities over the next 3 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 United States 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, over 3,000 additional travelers were denied travel here through this program in fiscal year 2015. 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 United States without a visa. We began to enforce these restrictions on January 21, 2016. Waivers from these restrictions will only be 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 United States. 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 5 years from traveling to the United States without a visa. In April, DHS began enforcing the mandatory use of high security electronic passports for all Visa Waiver Program travelers. In both February and June, CBP enhanced the ESTA application 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 4 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, we want to build more of these. In May 2015, I announced 10 additional airports in 9 countries that we've prioritized for preclearance. In May, CBP announced an "open season," running through August 1, for foreign airports to express interest in participating in the next round of preclearance expansion. I urge Congress to pass 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 fiscal year 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 have extensions, and 4 States or territories are out of compliance without an extension. Now that the final time table for implementation of the law is in place, we urge all States, for the good of their residents, to start issuing REAL ID-compliant drivers' licenses 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, to raise public awareness at sporting events. 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 home-grown, 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 last month, 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 Muslim 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. Last week, 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.

Finally, given the nature of the current threat from home-grown violent extremists, homeland security must include sensible gun control laws. We cannot have the former without the latter. Consistent with the Second Amendment, and the right of responsible gun owners to possess firearms, we must make it harder for a terrorist to acquire a gun in this country. The events of San Bernardino and Orlando make this painfully clear.

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 points. With the support of Congress we are surging resources and adding personnel to address the increased volume of travelers.

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 recent attacks, including those in Brussels and Istanbul.

As you know, in May of last year a Classified DHS Inspector General's test of certain TSA screening at 8 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 airport security. 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 are continuing 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 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.

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 two reprogramming requests that have enabled us to expedite the hiring of over 1,300 new TSOs, pay additional overtime to the existing TSO workforce, and 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.

We continue to encourage the public to join TSA PreCheck™. The public is responding. While enrollments a year ago were at about 3,500 daily, now enrollments are exceeding 15,000 a day. For 90% of those who are enrolled and utilize TSA PreCheck™, wait times at TSA checkpoints are 5 minutes or less.

Airlines and airports are also assisting to address wait times. We appreciate that major airlines and airport operators have assigned personnel to certain non-security duties at TSA checkpoints, and are providing support in a number of other ways. Longer term, we are working with airlines and airports to invest in "Innovation lanes" and other technology to transform the screening of carry-on luggage and personal items.

Our efforts are showing results. Nation-wide, the wait time for more than 99% of the traveling public is 30 minutes or less, and more than 90% of the traveling public is waiting 15 minutes or less. But we are not taking a victory lap. Over the Fourth of July holiday weekend, TSA screened 10.7 million travelers. June 30 and July 1 were the highest-volume travel days we have seen since 2007. During this period, however, the average wait time Nation-wide in standard security lines was less than 10 minutes, while those in TSA PreCheck™ lines waited an average of less than 5 minutes.

We plan to do more. The summer travel season continues, followed by holiday travel in the fall and winter. We are accelerating the hiring of an additional 600 TSOs before the end of the fiscal year. And we will continue to work with Congress to ensure TSA has the resources it needs in the coming fiscal years.

As I have said many times, we will keep passengers moving, but we will also keep them safe.

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.

On February 9, the President announced his "Cybersecurity National Action Plan," which is the culmination of 7 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.

We will collaborate with Underwriters Laboratory and others to develop a Cybersecurity Assurance Program to test and certify networked devices within the "Internet of Things"—such as your home alarm system, your refrigerator, or even your pacemaker.

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.

I have issued an aggressive time table 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. 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, 50% of Federal personnel are actually protected, including the Office of Personnel Management, and we are working to get all Federal departments and agencies on board by the end of this year.

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 97% of the Federal civilian government. 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 then before the directive.

Last month, 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. They will be released in final form later this year after public comment.

Finally, I thank Congress for passing the Cybersecurity Act of 2015. This new law is a huge assist to DHS and our cybersecurity mission. We are in the process of implementing that law now. 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.

I appreciate the additional authorities granted to us by Congress to carry out our mission. Today, we face increasing threats from cyber attacks against infrastructure

and I strongly believe that we need an agency focused on cybersecurity and infrastructure protection.

I have asked Congress to authorize the establishment of a new operational component within DHS, the Cyber and Infrastructure Protection agency. We have submitted a plan which will 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. I urge Congress to take action so we are able to ensure DHS is best positioned to execute this vital mission.

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.

Chairman MCCAUL. Thank you, Mr. Secretary.

The Chair now recognizes Director Comey for his testimony.

STATEMENT OF JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. COMEY. Thank you, Mr. Chairman, Mr. Thompson. My written statement has been submitted.

I think what I would do in just a few minutes is just highlight the way in which we in the FBI are thinking about the primary threat to the homeland, which comes at us in the form of the so-called Islamic State, the group that we call ISIL, and that is a threat that has 3 prongs. It is an effort by ISIL through their poisonous propaganda to motivate people to travel to their so-called caliphate; second, an effort to inspire those who don't travel to engage in acts of violence, especially directed at law enforcement or people in military uniform; and the third prong of that threat, which we talk about less, but we in this business focus on every day, are the directed efforts, that is, their efforts to send people to the United States to kill innocents or to specifically recruit and task people in the United States to kill innocents. Those are the 3 prongs of the ISIL threat.

There is good progress that has been made against the so-called traveler threat. Since last summer, we have seen a drop in the number of people attempting to travel to the so-called Islamic State. That may be a function of the fact that the message has gotten out that people will spend a long stretch in jail if they attempt to travel. It could also be a function of the fact that people have discovered that the so-called glory of the Islamic State is nothing but a mirage, and it is hell on earth. It could also be something that involves people staying home to try and do something on behalf of the Islamic State. So we don't take great comfort in a drop in the number of travelers.

The second prong is the one that dominates our lives today. As Secretary Johnson mentioned, there are hundreds of people in the United States who are consuming the propaganda of this so-called Islamic State and being motivated to move toward violence. Our job together is to find those needles in a haystack. In fact, our job is harder than that. It is to find pieces of hay in that haystack that may become a needle and disrupt them before they move from consuming to acting on that poisonous propaganda.

Those are—and the most painful examples of that recently, obviously, are Orlando and San Bernardino, but there are plenty of others around this country. We have arrested 4 just in this month to disrupt them, people who are moving on that path from consuming to acting on violence.

The last prong, as I said, is one we never take our eye off, for the reasons you mentioned, Mr. Chairman. We all know there will be a terrorist diaspora out of the caliphate as military force crushes the caliphate. Those thousands of fighters are going to go someplace, and our job is to spot them and stop them before they come to the United States to harm innocent people.

I am lucky to lead an organization like the FBI that is made up of great men and women who do this all day every day, and to do it in partnership with the kind of people sitting at the table here and the people who they represent. We are doing our absolute best against a threat that is difficult to see and to stop. I am very proud of the work we have done today, and it will continue.

I also didn't know this was Secretary Johnson's last appearance. I have 7 years left in my term, so I will be back. I just want to say what a pleasure it has been to work with my old friend, not that you are old, but my friend from many years ago, and to see what he has done at that great organization.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Comey follows:]

PREPARED STATEMENT OF JAMES B. COMEY

JULY 14, 2016

Good afternoon Chairman McCaul, Ranking Member Thompson, 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 including terrorists' use of technology to both inspire and recruit. The widespread use of technology permits terrorists to propagate the persistent terrorist message to attack U.S. interests whether in the homeland or abroad. As the threat to harm our 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 with me today are the Department of Homeland Security and the National Counterterrorism Center with whom we work 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 threat posed by foreign fighters, including those recruited from the United States, traveling to join the Islamic State of Iraq and the Levant ("ISIL") and from home-grown violent extremists are extremely dynamic. The tragic event in Orlando last month 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 on-going investigation has developed strong indications of radicalization by this killer, but further investigation is needed to determine if this attack was inspired by foreign terrorist organizations. 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. Our work is very challenging: We are looking for needles in a Nation-wide haystack, but even more challenging, we are also called upon to figure out which pieces of hay might someday become needles. That is hard work and it is the particular challenge of identifying home-grown 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 home-grown vio-

lent 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. Terrorists 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 the individuals cannot travel, the terrorists 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 wide-spread reach through the internet and social media is most concerning as the group has proven dangerously competent at employing such tools in furtherance of its nefarious strategy. ISIL uses high-quality, traditional media platforms, as well as wide-spread social media campaigns to propagate its extremist ideology. Recently released propaganda has included various English language publications circulated via social media.

Social media is used as a tool for groups such as ISIL to spot and assess potential recruits. With greater access to social media platforms, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the United States either to travel to engage in terrorist organization activities or to conduct a homeland attack. Such use of the internet, including social media, in furtherance of terrorism and other crimes must continue to be addressed by all lawful means, while respecting international obligations and commitments regarding human rights (including freedom of expression), the free flow of information, and a free and open internet.

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, not necessarily with the initial intention to participate in terrorist activities. 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 in Western countries. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers. The challenge here is how to defeat ISIS and thwart its use of the internet for terrorist and other criminal activity while continuing to help the internet be a force for good that promotes the enjoyment of freedom of expression, association, and peaceful assembly—especially for individuals who are acutely at risk.

Some of these conversations occur openly on social networking sites, but others take place via private messaging platforms that use encryption. Terrorists' exploitation of encrypted platforms presents serious challenges to law enforcement's ability to identify, investigate, and disrupt terrorist threats. We respect the 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, because the free flow of information is vital to a thriving democracy.

The United States believes that the internet has been, and will be, a tremendous force for good—it has enabled the promotion and protection of fundamental freedoms. But the internet's potential is dependent on people's ability and willingness to use it without undue restrictions and fear. Individuals must be able to trust that there will be respect for privacy, access to information, and freedom of expression, and there will be appropriate legal restraints on Government action. Without these protections, the internet risks becoming a mechanism for social control, rather than a place for all to express and exchange ideas, views, and information. The risks posed by terrorism are great, and the need for law enforcement is strong, but we must balance those requirements against the important role played by free expression in helping to address those same challenges.

The benefits of our increasingly digital lives, however, have been accompanied by new obstacles and, accordingly, we are considering 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. The decisions we make over the next several years about the future of the internet—including the laws and policies that are put in place to protect freedom of expression while thwarting terrorist and other criminal activities—will determine whether our children will continue to enjoy an open, interoperable, secure, and reliable internet.

This in turn will greatly affect whether the internet will continue to yield the remarkable social, economic, and political progress that it has to date.

We must ensure both the 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, those changes also hinder efforts 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 on-going, 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. Along with our domestic and foreign partners, we are collecting and analyzing intelligence about the on-going threat posed by foreign terrorist organizations and home-grown 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. 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, and while we are making progress, we still have more work to do. Our goal every day is to get better at using, collecting, and sharing intelligence to better understand and defeat our adversaries.

We have established an Intelligence Branch within the FBI to lead integration across the organization, with responsibility for all intelligence strategy, resources, policies, and functions. The branch is headed by an Executive Assistant Director who looks across the entire enterprise and drives integration. We have also established a Bureau Intelligence Council within the Intelligence Branch to ensure we take a consolidated and integrated approach to threats. As part of this council, senior-level intelligence professionals will lead enterprise-wide strategic assessments, facilitate a broader understanding of how threats mitigated across operational programs are related, and help balance our priorities with those of the broader intelligence community and U.S. Government.

We have also put in place training for all levels of the workforce, from entry-level employees to senior leaders, to ensure we achieve that integration throughout the enterprise. New agents and analysts now engage in practical training exercises and take core courses together at the FBI Academy—and, as a result, are better prepared to collaborate effectively throughout their careers. In addition, all field supervisory agents, supervisory analysts, and foreign language program managers, as well as headquarters unit chiefs, now attend a 2-day forum focused on sharing best practices to advance integration. All section chiefs and GS–15 field agents and analysts also attend a 2½-day course on effectively integrating intelligence processes to maximize resources against prioritized threats. Finally, our entire executive management team at headquarters has participated in two integration sessions to ensure the integration of intelligence into every aspect of the FBI's work.

In addition, we are dedicated to expanding the developmental and leadership opportunities for all members of the intelligence program workforce. We recently put in place 7 additional Senior Supervisory Intelligence Analyst positions in various offices around the country to increase leadership opportunities for our analyst cadre and enhance our management of field intelligence work. These GS–15 analysts manage intelligence in the field, fulfilling a role that has traditionally been performed by agents and demonstrating we are promoting effective integration throughout the organization.

We have also redesigned the training curriculum for another part of the Intelligence Program workforce—Staff Operations Specialists ("SOSs")—to aid in their performance of tactical functions in the field. In addition, a new development model clearly identifies SOS work responsibilities, tasks, training, and opportunities at the basic, intermediate, and advanced levels to guide the professional growth of SOSs across the organization at all points throughout their FBI careers.

Similarly, our language workforce continues to make important contributions to the mission. Our language professionals have recently supported numerous important investigations and operations, including Malaysia Airlines Flight 17 last summer, numerous ISIL-related investigations, the disruption of a nuclear threat in Moldova, and so many others. The National Virtual Translation Center ("NVTC") also continues to provide excellent service, supporting hundreds of Government offices each year.

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. Toward 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 priorities for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

CYBER

Virtually every National security and criminal threat the FBI faces is cyber-enabled in some way. We face sophisticated cyber threats from foreign intelligence agencies, hackers for hire, organized crime syndicates, and terrorists. These threat actors constantly seek to access and steal Classified information, our trade secrets, our technology, and our ideas—things of incredible value to all of us and of great importance to our National and economic 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 Federal Government view improving cybersecurity and preventing 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 organized crime syndicates, as well as the most prolific botnets. We need to be able to move from reacting to such malicious activity after the fact to preventing such attacks. That is a significant challenge, but one we embrace.

As the committee is well aware, the frequency and impact of malicious cyber activity 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, which is malicious software that takes control of victims' computers and systems and encrypts the data until the victims pay a ransom. Last year alone reported losses from ransomware totaled more than $24 million. The FBI works closely with the private sector so that companies may make informed decisions in response to ransomware and other 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 encourage payment of ransom, as payment of extortion monies may encourage continued criminal activity and paying a ransom does not guarantee that an organization will regain access to its data.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and information sharing inside and outside of Government, to our emphasis on developing and retaining new talent and changing the way we operate to defeat these threats. 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 cyber space.

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 McCaul, Ranking Member Thompson, 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.

Chairman MCCAUL. Thank you, Director Comey.

The Chair now recognizes Director Rasmussen.

STATEMENT OF HONORABLE NICHOLAS J. RASMUSSEN, DIRECTOR, THE NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. RASMUSSEN. Good morning, Chairman McCaul, Ranking Member Thompson, and Members of the committee. I appreciate the opportunity to join my colleagues Secretary Johnson and Director Comey here this morning to talk about the threats that worry us the most.

I would also like to thank you, Mr. Chairman, for your recent visit to address my work force at NCTC in a town hall setting. It was a terrific, terrific session, and I appreciate the support that your committee and you personally have shown to our work force and to our mission.

As Director Comey and Secretary Johnson said, the attack in Orlando underscores the critical nature of our collective vigilance against home-grown violent extremism. Looking ahead, we certainly expect that more additional home-grown violent extremists will try to replicate the violence and potentially capitalize on media attention that came from attacks like those like the one in Florida generated. It is clearly the case that, in the past few years, the pool of potential home-grown violent extremists has expanded significantly. As Director Comey has talked about in prior testimony, the FBI has investigations across all 50 States that touch on this population.

This increase in caseload tracks with ISIL's rise in prominence in the large-scale media and propaganda apparatus that it has tried to development to influence populations around the world. As we approach 15 years after the 9/11 attacks, I would say it is fair to say that the array of terrorist actors around the globe is broader, deeper, and wider than it has been at any time since 9/11. It is ISIL's narrative, rooted in unceasing warfare against all that it defines as its enemies that also extends well beyond the Syria and Iraq battlefield. ISIL has carried out attacks ranging in tactics and targets, from the downing of a Russian airliner in Egypt to the attacks last November in Paris against restaurants, a sports stadium, and a concert venue, attacks on an airport in Brussels—in both—in Brussels and Istanbul—and, most recently, the killing of hostages and law enforcement officials in a cafe in Bangladesh. All of these attacks show how ISIL can draw upon local individuals, local affiliates to carry out these lethal attacks.

So this array of recent attacks that I just rattled through demonstrates that the threat landscape is in many ways less predictable than ever. While the scale of the capabilities currently dem-

onstrated by most of the terrorist actors that we are dealing with does not rise to the level of the capability that core al-Qaeda had to carry out catastrophic attacks on 9/11, it remains fair to say that we face more threats originating in more places involving more individuals than at any period since 9/11.

It is ISIL's access to resources and territorial control in areas of Syria and Iraq that are key ingredients to the group's development of external operations capability, which includes the group's ability to threaten the homeland. For that reason, shrinking the size of that territory controlled by ISIL, denying ISIL access to additional manpower in the form of foreign fighters remains a top priority. Success in these areas is essential to our ultimate effort to prevent the group from operating on a global scale as a terrorist organization.

Clearly, progress has been made in these areas, 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 current tempo of ISIL-linked terrorist activity is a painful reminder ISIL's global reach.

It is important to understand that we do not judge that there is a direct link between the group's current battlefield status on the ground in Iraq and Syria and the group's capacity to operate as a global terrorist organization with capabilities around the world. ISIL's external operations capability has been building and entrenching during the past 2 years, and we don't think that battlefield reverses alone in Iraq will be sufficient to degrade that terrorism capability that has evolved with ISIL.

So, without question, the tremendous efforts we are making as a Government to counter ISIL are absolutely warranted, but I want to shift briefly for a moment to stress that we still regard al-Qaeda and al-Qaeda's various affiliated organizations as a principal counterterrorism priority, and we are particularly concerned about al-Qaeda's growing safe haven in Syria.

We know that ISIL is trying to strengthen its global network by relocating some of its remaining leadership from South Asia to Syria, and these leaders include individuals who have been part of the group since the time even before 9/11. Now that many of them are in Syria, we believe that they will work to threaten the United States and our allies.

Turning to broader trends in the contemporary threat environment, I will briefly highlight three that concern us the most. The first trend is the persistent effort by our terrorist adversaries to target the aviation sector. While there is much more I could say in a Classified setting on this, I can say here that both al-Qaeda and ISIL remain focused on defeating our defenses against aviation-related attacks.

The second trend I would highlight is the increasing ability of terrorist actors to communicate with each other outside our reach through the use of encrypted applications.

Third, while we have seen a decrease in the frequency of large-scale, complex plotting efforts that sometimes span several years, we are instead seeing proliferation of more rapidly evolving and maturing threats, the so-called flash-to-bang ratio that we have talked to this committee before about. The time between when an

individual first decides to pursue violence and when an actual attack might occur has become extremely compressed, placing much greater pressure on law enforcement and intelligence.

In our environment, our best hope of providing enduring security in this environment rests on our ability to counter the appeal of terrorism and dissuade individuals in the first place, and that goes to the subject of countering violent extremism, which was something raised by both the Chairman and the Ranking Member.

NCTC, working with DHS and FBI, has developed CVE tools to build community resilience across the country, but there is clearly more work to be done by all of us together in this environment, and I look forward at NCTC to our doing our part.

Thank you, Mr. Chairman.

Thank you, Ranking Member, and Members of the committee.

I look forward to taking your questions.

[The prepared statement of Mr. Rasmussen follows:]

PREPARED STATEMENT OF NICHOLAS J. RASMUSSEN

JULY 14, 2016

Thank you, Chairman McCaul, Ranking Member Thompson, 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).

Over 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-Qaeda 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 recent wave of attacks in Bangladesh, Iraq, Saudi Arabia, and Turkey. As these attacks demonstrate, ISIL's strategy is to weaken the resolve of its adversaries and project its influence world-wide 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, we are no doubt reminded by the shooting in Orlando, Florida, last month that home-grown 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

The attack in Orlando underscores the importance of what we are here today to discuss and the critical nature of our vigilance against home-grown violent extremism. While the reasons for the attack in Florida become known and continue to inform how we detect and respond to these types of incidents, 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 and attention that attacks like the one in Florida 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 summer holidays and the large public events, celebrations, and gatherings that accompany them. 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 said, the FBI has investigations on around 1,000 potential HVEs across all 50 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 world-wide. What we have seen over time is that HVEs—either lone actors or small insular groups—continue to gravitate toward simple tactics that do not require advanced skills or outside training. The majority of HVEs will likely continue to select traditional targets, such as military personnel, law enforcement, and other symbols of the U.S. Government. 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.

As we approach 15 years 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 Bangladeshi law enforcement officials in a cafë in Bangladesh; and the bombing of a crowded commercial district in Baghdad—all of which demonstrate how ISIL can capitalize on local affiliates 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-Qaeda 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 recently saw at Istanbul's Ataturk Airport and the attack in Belgium in March, terrorists remain focused on attacks against aviation 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. World-wide 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 and its infrastructure for 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 it is not always clear; sometimes ISIL members in Iraq and Syria reach out to individuals in the homeland to enable others 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's development of an external operations capability, to include their ability to threaten the homeland. For that reason, shrinking the size of territory controlled by ISIL, and denying the group access to additional manpower in the form of foreign fighters and operatives, 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. 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 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 2 years, and we do not think battlefield losses alone will be sufficient to degrade completely the group's terrorism capabilities. As we have seen, the group has launched attacks in periods in which the group held large swaths of territory as well as during the past few weeks, as the group feels increasing pressure from the counter-ISIL campaign. In addition to their efforts to conduct external attacks from their 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.

ISIL spokesman Abu Muhammad Adnani's most recent public statement—which encourages ISIL supporters in the United States to conduct attacks in their home countries instead of traveling to Iraq and Syria—may suggest that ISIL recognizes the difficulty in sending operatives to the homeland for an attack. ISIL likely views

the United States as a harder target than Europe due to Europe's proximity to the conflict. U.S. ports of entry are under far less strain from mass migration, and U.S. law enforcement agencies are not overtaxed by persistent unrest, as some of our counterparts are overseas.

In Europe, we are concerned about ISIL's demonstrated ability to conduct coordinated attacks by deploying operatives from Syria and Iraq and leveraging European jihadist networks. 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 their 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 U.S. 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.

Similar to the HVE challenge we face, Europe-based individuals have responded to ISIL's violent message and act on the group's behalf. A violent extremist attacked a police officer and his wife last month in France and pledged his allegiance to ISIL amir Abubakr al-Baghdadi during the hostage situation through a live-streaming social media service.

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 to entering the United States via the U.S. Refugee Admissions Program. Specifically, applicants have little-to-no control as to whether the United Nations will refer them for consideration by the U.S. Refugee Admissions Program. Those refugees who are referred to the U.S. Refugee Admissions Program are then subjected to a process for resettlement of refugees administered by the United Nations High Commissioner for Refugees (UNHCR).

To ensure proper scrutiny of refugee applicants referred to the United States 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 comprehensive system of checks—including the participation of the Departments of Homeland Security, State, Defense, and the FBI as well as additional 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 U.S. 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 intelligence community (IC) holdings to then validate those findings.

The second way is our screening against IC holdings. We screen applicant biographic information against the IC holdings to identify any possible matches to raw intelligence reporting and then conduct 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-Qaeda and the various al-Qaeda 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 AQAP 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-Qaeda 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-Qaeda still figures prominently in that analysis.

We are particularly concerned about al-Qaeda's safe haven in Syria because we know al-Qaeda 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-Qaeda affiliate there—the Nusrah Front—to threaten the United States and our allies.

The Nusrah Front is al-Qaeda's largest affiliate and one of the most capable armed groups operating in Syria. Its integration of al-Qaeda veterans provides the group with strategic guidance and enhances its standing within the al-Qaeda global movement. In April, the U.S. military successfully targeted some of the Nusrah Front's senior members, including long-time al-Qaeda member and former spokesman for the group in Syria, Abu Firas al-Suri. We will remain vigilant in our efforts to counter this group and the threats it poses to the West.

We believe we have constrained the group's effectiveness and their ability to recruit, train, and deploy operatives from their safe haven in South Asia; however, this does not mean that the threat from core al-Qaeda in the tribal areas of Pakistan or in eastern Afghanistan has been eliminated. We assess that al-Qaeda 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-Qaeda will remain a threat. Al-Qaeda'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 to the level of risk the United States may face over time if al-Qaeda regenerates, finds renewed safe haven, or restores lost capability. We are very much on alert for signs that al-Qaeda'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 U.S. Government will retain sufficient capability to continue to put pressure on that core al-Qaeda network and therefore reduce the risk of a resurgence by al-Qaeda 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-Qaeda. 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, they can be effective, especially if they believe 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.

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 will be led by the Department of Homeland Security for the first 2 years; afterward, the Department of Justice will assume leadership. It will be staffed by multiple departments and agencies, including the FBI and NCTC. The main objectives of the task force are to coordinate Federal support for on-going 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 United States, 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 table-top 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 McCaul, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to testify before you this morning. As we are reminded by the events in Florida as well as globally just a couple of weeks ago, 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 over the months and years to come in order to continue to protect the homeland.

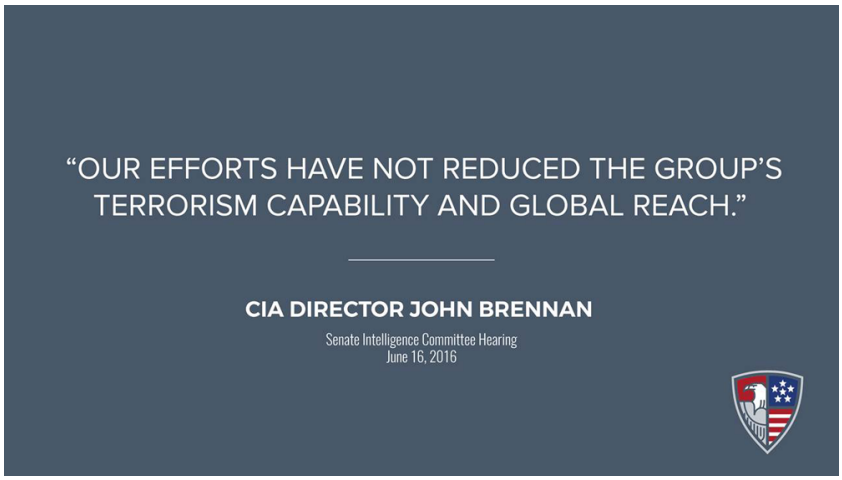
Thank you all very much, and I look forward to answering your questions.

Chairman MCCAUL. Thank you, Director.

I now recognize myself for questions.

There are some who argue that our military actions in Iraq and Syria have diminished the threat to the homeland, and I think, Director Rasmussen, you touched upon this. However, the CIA director, John Brennan, just recently in his testimony gave the administration a failing grade in the fight against ISIS and said, "Our efforts have not reduced the group's terrorism capability and global reach."

[The information follows:]



Chairman MCCAUL. I want to ask this question to each of you, starting with Secretary Johnson. Do you agree with the CIA director's comments?

Secretary JOHNSON. I haven't read Director Clapper's—I mean, Director Brennan's testimony in its entirety. I have seen excerpts of it.

The way I would assess it is we are making significant progress in ISIL's ability to maintain any type of caliphate in Iraq and Syria. I think any time a terrorist organization from the homeland security perspective is able to establish a caliphate, that has real implications and troubling implications. We have made progress there in our ability to roll back their territory, degrade their ability to finance, degrade their ability to communicate.

I agree with Nick's assessment, however, that we have—ISIL's ability to conduct external attacks, to inspire, to self-radicalize is still very much present, and that is something that we need to continue to focus our U.S. Government National security, homeland security resources on. In no respect, I think, are we satisfied that their ability to engage in external attacks and self-radicalize actors and inspire actors has been diminished to the point where we can step back and take a breather. We have to stay focused on that very much so.

Chairman MCCAUL. Director Comey.

Mr. COMEY. I agree with what Secretary Brennan—excuse me—Director Brennan said. The intelligence community assesses that, as the caliphate is crushed, the so-called Islamic State will become more desperate to demonstrate its continued vitality, and that will likely take the form of more asymmetric attacks, more efforts at terrorism. So I agree with Secretary Johnson. It is necessary to crush the caliphate, but we can't take our eye off what the next move will be by these killers.

Chairman MCCAUL. Director Rasmussen.

Mr. RASMUSSEN. I guess the way I would think about it, Mr. Chairman, is that one shouldn't necessarily expect that there is a one-for-one correlation between progress on the ground in Iraq and

Syria, which is undeniable and is essential to our long-term effort to crush ISIL or to defeat ISIL, but one shouldn't expect a one-for-one correlation between that effort and the results we are seeing on that front and near-term shrinkage of this external operations capability that the group has invested in over time. So I would consider that as something that is going to lag. Our success in this area is going to take longer and require more effort.

Chairman MCCAUL. The next question, we have been long worried about ISIS' internet directives to kill both military and police officers in this country. After Dallas and the tragic events there—I was born and raised in that city—we now see a new threat to law enforcement from another direction that I see—this, I am concerned about—from fringe groups out there. I direct this to Secretary Johnson and Director Comey.

As we look at the upcoming Republican Convention—and I will be attending on Monday—can you comment on the threat from these fringe groups? I know some have directed people to come to Cleveland and bring your weapons. Obviously, there is great concern among the American people of the status of security at that convention.

Secretary Johnson, can you comment on that?

Secretary JOHNSON. Well, I am concerned about the prospect of demonstrations getting out of hand. I am concerned about the possibility of violence. We have within DHS some 3,000 personnel that will be dedicated to the security of the Republican National Convention and the Democratic National Convention each, consisting of Secret Service, TSA, Homeland Security Investigations, Customs and Border Protection, NPPD, Coast Guard. I know that there will be at least another 1,000 or so U.S. Government personnel at hand in both places, a number in Cleveland of the Ohio Guard, as well as probably thousands in terms of State and local law enforcement.

We have been planning and preparing for both conventions now for over a year. As I mentioned earlier, I plan to inspect the security at both sites; Cleveland tomorrow, Philadelphia next Friday.

So I think we have to be concerned about things getting out of hand, very definitely, but there will be a lot of security and lot of preparation in place. There is a certain level of First Amendment protected activity that is guaranteed to demonstrators at National political conventions. It will be confined. It will be roped off in an isolated area, but it is something that we will have a lot of security devoted to, Mr. Chairman.

Chairman MCCAUL. Thank you.

Director Comey, to the extent you can in an open setting, can you talk about the nature of the threats, threat streams you see out there to this convention?

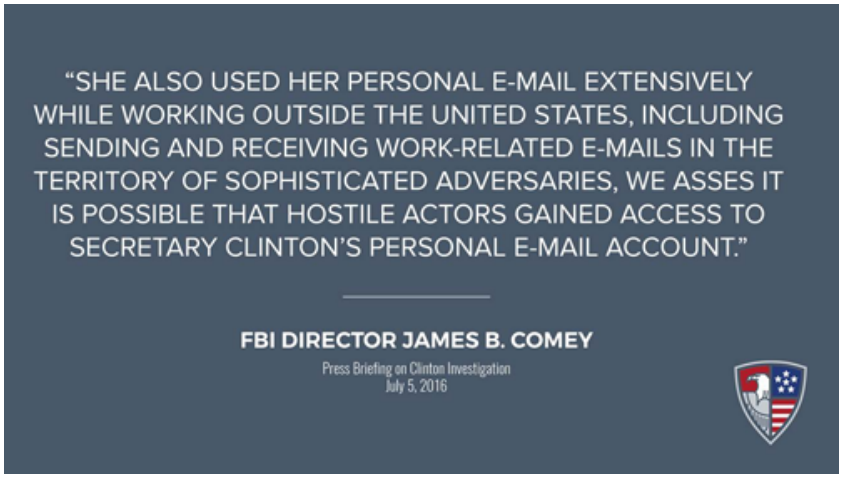
Mr. COMEY. Yes, Mr. Chairman. The definition of domestic terrorism is someone who engages in acts of violence directed against other people in order to coerce a civilian population or try and coerce a government, and so, any time there is a National spotlight on a political event in the United States, there is a risk that groups that aspire to do just that, to engage in acts of domestic terrorism, will be attracted.

It is a threat we are watching very, very carefully. It is the reason we have hundreds of people focused on intelligence and de-

ployed to Cleveland. I don't want to talk about particular groups here, but there is a concern any time there is an event like this that people from across a spectrum of radical groups will be attracted to it, so we are watching it very, very carefully.

Chairman MCCAUL. Thank you. Last question. I want to ask you about the National security implications of Secretary Clinton's private server. You stated that she used personal emails extensively while outside the United States, including sending and receiving work-related emails in the territory of sophisticated adversaries. Given that, you assessed it is possible that actors gained access to her personal email account. I know when we travel overseas, we are told not to bring these devices into nations with foreign adversaries.

[The information follows:]



Chairman MCCAUL. You went on to say that 7 of her email chains concerned matters classified at Top Secret but also special access programs that were sent and received. Those programs were designed in part to protect the country's most highly classified and sensitive information.

Can you tell us, if her private server, if these emails were breached, what would be the National security implications to that, and could American lives be at risk?

Mr. COMEY. Thank you, Mr. Chairman. I was hoping to talk about terrorism, but I will do my best to address this in an open setting.

As I have said publicly, I don't know—we don't have direct evidence that the server was successfully hacked. We wouldn't, though, expect to see that evidence from sophisticated adversaries, given the nature of the adversary and given the nature of the system.

The definition of Classified information is it is information that an intelligence agency assesses the improper release of which would cause some damage to the United States.

I can't answer the question beyond that without going into the specifics of the emails, which I can't do in an open setting.

Chairman MCCAUL. I know we can't talk about what special access programs were on these emails in the server. You and I know how sensitive they are. I hope and pray that they were not compromised.

With that, the Chair recognizes the Ranking Member.

Mr. THOMPSON. Thank you, Mr. Chairman.

Director Comey, as America's top cop, I want you to appreciate my question as it relates to the access to guns in this country by dangerous people. The International Association of Chiefs of Police, the Major Cities Chiefs Association, and other groups representing law enforcement are supportive of sensible gun laws, including the broadening of background checks, and I am talking about the Charleston loophole. We are told that, with the 3-day requirement, that if your department hadn't completed the check, that person can automatically get a gun. What are your thoughts on that loophole?

Mr. COMEY. Well, thank you, Mr. Thompson. I can answer factual questions. The Bureau does not get involved in policymaking or recommending legislation, so that is—issues like that should be directed to the Department of Justice.

The way that the law works is, after 3 days, if we have not denied the transaction by finding some prohibition, the retailer may transfer the weapon. Now, large retailers like Walmart will not, they wait for an affirmative clear from the FBI, but smaller retailers, for economic reasons that I understand, will frequently transfer in the absence of a no, and so that is what happened in Charleston.

Mr. THOMPSON. So I guess your testimony is smaller retailers, because of capacity or otherwise, sometimes approve purchases of guns, like in the Charleston incident, that, under normal circumstances, would have been—that individual would have been prevented from purchasing that gun?

Mr. COMEY. Right. The case in Charleston was that killer should not have gotten access to that gun because there was documented evidence that he was a drug user. At a larger retailer, as a matter of discretion, they would not have transferred the gun until they heard back affirmatively it is OK from the FBI. The smaller retailers, because each individual sale may be more important to them than a bigger company, will likely transfer. That is the most common case.

Mr. THOMPSON. Thank you very much.

Secretary Johnson, you have stated that we must make it harder for a terrorist to acquire guns in this country. A lot of us are concerned about the assault-style, military-grade weapons, which generally is a weapon of choice for, like, Orlando and other situations. Have you thought how Congress could make it harder for these international or domestic terrorist individuals to acquire guns?

Secretary JOHNSON. Yes. I believe that, consistent with the Second Amendment, as interpreted by the Supreme Court and consistent with a responsible gun owner's right to own a gun, we can and we should make it harder for a terrorist to obtain a gun to commit a terrorist act. There is legislation now in Congress, sponsored by Senator Feinstein and others, and then there is an alternative approach, sponsored by Senator Collins and others, that

would give the Attorney General added discretion to deny a gun purchase if somebody is on one of the various lists. I think that that is a sound approach. I think that we should provide the Attorney General with that added discretion, along with some form of an adjudication process to adjudicate the denial if the attempted gun purchaser chooses to do so.

So I think that—I encourage Congress to wrestle with this issue, wrestle with these proposals, because I think that it is not just a matter of public safety that we do this, it is now a matter of homeland security that we make it harder for a terrorist to acquire a gun.

Mr. THOMPSON. Thank you.

Director Comey, your website: "Don't Be A Puppet". I understand that you established this to educate school-age children about the threat of violent extremism. Not surprisingly, law enforcement officers have looked at it also.

Can you tell me how that website has—has it accomplished what you wanted to? Are there some other things you would like to do to get the community engaged in helping identify some of these extremist groups?

Mr. COMEY. Thank you, Mr. Thompson. The website "Don't Be A Puppet" is designed in a way we hope will be more attractive for kids, who are looking for something a little cooler than the FBI normally throws out, to explore the ways in which extremist groups, both radical Islamic groups and other extremist groups, might try to recruit them or lure them. So it is a series of games and interactive events on the website that allow them to go in and explore and learn from it.

We have gotten great feedback from around the country. We invited a lot of people to give us input before we rolled it out. We have gotten great feedback from teachers especially that they like it, that the kids—the kids, I think their grade for us is about a B. They think we could be a little cooler, but we have stretched as far as we could stretch right now in the coolness department, and it is—we are getting great feedback. So we will continue to watch it and see.

There are plenty of other things we are doing. The Department of Homeland Security is doing a ton of things. There is always more we can do.

Mr. THOMPSON. Thank you.

Last question. Director Rasmussen, the attack in Bangladesh illustrates that ISIS will threaten Westerners outside of the Middle East. Are soft targets, such as cafes in Bangladesh or a club in Orlando, the new battlefield in which Americans should expect ISIS to attack? If so, what can the United States do to counter this type of terrorist activity?

Mr. RASMUSSEN. Thank you, Mr. Thompson. I guess I would highlight two things that we can do to try to counter this kind of vulnerability when Americans are traveling or living overseas. The first is just being as open and transparent with the American people as possible about the risks we see in overseas locations. We work very closely with the State Department to provide them the intelligence they need to make sound, sensible judgments about

travel warnings and travel alerts for Americans who are going overseas or living overseas.

Beyond that, though, I would say our best hope is to work with local partners to buildup their capacity, to increase the capacity of local law enforcement, local military authorities to respond to and to prevent—local intelligence authorities to respond to or prevent these kinds of acts of terror. As you can imagine, if you think about all the different places around the globe where ISIL has been active, that is a mixed story. In some cases, we have very, very capable partners overseas with whom we can work very closely. In other cases, those partners have a lot of challenges and suffer from a lot of capacity deficits that we are going to have to work out over time.

Mr. THOMPSON. Thank you. I yield back.

Chairman MCCAUL. I thank the Ranking Member.

The gentlemen from New York, Mr. King, is recognized.

Mr. KING. Thank you, Mr. Chairman.

Let me thank all the witnesses for their testimony and for their service.

Secretary Johnson, when you said you were—wondering what keeps you awake at night, I thought you were going to say it was testifying before Congress, because that would—again, thank you for your service.

Director Comey, I would like to discuss Orlando with you, not for the sake of Monday morning quarterbacking but planning toward the future. The investigation was stopped by the FBI based on the criteria at the time that he did not seem at all sophisticated; he didn't know the difference between Sunni and Shia; didn't seem to have any formed ideology at all.

Based on what we know now about the profile that ISIS is looking for—in some cases, the person who is deranged, the person who may be influenced by Islamist ideology, and whether or not he is Islamist himself, whether he even fully appreciates it—I would ask going toward the future, how long investigations can be kept open? I think basically it is a 6-month investigation now, and then it either has to be stopped or get extended. Can there be an indefinite period where the local police would be brought more into it? I mean, obviously, you don't have the personnel to be carrying out surveillance all over the country or to be following people, but if you have local police, detectives, undercovers, informers, sources, if it could be handed off for a period of time to the local police, they can say: Here is a person who doesn't meet the threshold of terrorism. We don't have enough to keep a formal investigation open, but can you keep an eye on him, or can you report back to us on him?

I am thinking like, for instance, in New York City, you probably have more cops than FBI agents in the whole country, or take Chicago, with a large police force, and others. So could better use be made of local law enforcement, and could these people who are in sort of a twilight zone between terrorism and maybe just being dysfunctional citizens, that local police could be really kept apprised, and they ought to in turn keep you apprised?

Mr. COMEY. Yes. Thank you, Mr. King. That is a very good question. The answer is I don't know yet, although we are having those conversations with our State and local partners.

The way it works in the FBI is a preliminary investigation stays open for 6 months, and then it can be extended in the local field office for another 6 months. It can be extended after that; it just requires higher level of approvals.

What happens with preliminary investigations is it is designed to figure out, is there anything here? If there is, we convert it to a full investigation. If the preliminary rebuts the initial allegation, then we close it.

Our local partners have asked, is there some way that, in addition to us being on the joint terrorism task forces, where they see all the cases we open and close, is there something else we might be able to do to flag a person? That is a knotty question, but it is one that is a serious question, so we are working through that right now. I don't know, but it is worth a conversation.

Mr. KING. I also think in terms of the Boston Marathon bombing where the older Tsarnaev brother, you know, nothing in the preliminary investigation showed anything, but if the local police had been aware of it, they may have heard of what he was saying in the mosque, the fact that he was thrown out of the mosque for some of his conduct, and that could have, you know, reopened the full investigation.

So, again, to the extent you can use local police, I think it is really essential, because they are really certainly an added element, and, again, they would have sources just by the nature of being local cops that may not be available at the Federal level.

Secretary Johnson, I know that your Department has been aggressively exploring the use of social media. Can you give us the status of those efforts? Do you feel you have sufficient resources to do what you want to do as far as vetting, as far as employees, as far as immigrants to go forward?

Secretary JOHNSON. We use social media for something like 30 different purposes across the Department. We have expanded the use of social media when it comes to immigration reviews, immigration benefits.

What I would like to do is build a centralized social media center for excellence, which will be housed in our National Targeting Center in CVP. We have a reprogramming request pending right now with Congress to help fund that. In the outyears, I would like to see Congress do a bit more to help us out with a centralized social media capability. Right now, a lot of that is done for USCIS, but as I am sure you know, CIS is a fee-based organization. So there are enough purposes for social media across our entire Department that I want to see this capability expanded and funded. So we have the reprogramming request now, and we could use more money in the future years.

Mr. KING. Secretary, I have been a supporter of DHS grant programs. I can tell you, though, on the floor of the Congress, there is concern among a good number of people about the CVE grants, that they may go to an organization like CAIR, which has been an unindicted co-conspirator and which I understand the FBI is still

not allowed to deal with. Is there any assurance you can give us that those grants would not go to an organization like CAIR?

Secretary JOHNSON. There will be a security review conducted with respect to each potential grantee before we grant out any money.

Mr. KING. But——

Secretary JOHNSON. This is a new program. We just announced notice of the proposal out to the public, solicitation out to the public last week, but there will be a security review in connection with every grant.

Mr. KING. But being an unindicted co-conspirator in one of the largest money-laundering terrorist cases in the country, shouldn't that be sufficient grounds to deny a grant?

Secretary JOHNSON. Without knowing the specific case, that seems likely, yes, sir.

Mr. KING. It was the Holy Land Foundation case. My understanding is the FBI still will not deal with CAIR because of that.

Director Comey, is that true?

Mr. COMEY. That is correct.

Mr. KING. Thank you. I yield back.

Chairman MCCAUL. The Chair recognizes Ms. Sanchez.

Ms. SANCHEZ. Thank you, Mr. Chairman.

I want to thank all of the gentlemen before us today for all the great work that you are doing.

Secretary Johnson, in March, you came before our committee, and we were discussing the countering violent extremism mission, and we talked about having the Department of Homeland Security allowing some of those grants to be used to nonprofit organizations to help us in countering the fight and going after the fight against terror. I just want to thank you and compliment you, because I know that you are finding new and innovative ways to include those nonprofits that we have in our area. As you know, I have one of the largest Muslim and Arab communities in our Nation, so we work very closely with a lot of our nonprofits to keep an ear to the ground and to ensure that we are on the forefront of trying to eliminate any of this radicalization that has such a potential, as we saw in San Bernardino.

I want to ask a couple of questions. The first would be, after 9/11, we tried to share more information between local, State, and Federal agencies, especially in the intelligence gathering and sharing. So I wanted to ask you a little bit about, is that working? Are we going to open up more or eliminate more silos? What more can we do to ensure now, as we see really the front line of information, as we saw in Los Angeles, for example, when somebody saw something, phoned it in, and our local enforcement was able to get to some bomb-making materials and other things that a gentleman had, how can we help to ensure that information is shared, or is there enough going on at this point? I would ask any of you.

Secretary JOHNSON. I will start. My general assessment is that we are doing much better now than we used to through JTFs, through joint intelligence bulletins, through fusion centers, through our own personal relationships working together. Jim and I, for example, had been on conference calls with literally hundreds of

State and local law enforcement personnel to share what we are seeing here at a National level.

In terms of the public's sharing information with us, that is a work in progress. It is almost always the case that when somebody self-radicalizes, there was somebody else that saw the signs. So we all from the homeland security perspective and the law enforcement perspective need to continue to encourage the public: If you see something, say something. But in terms of our own information sharing in law enforcement, I think we are on the right track, and I think we are much better than we used to be.

Ms. SANCHEZ. Good. I have a question for you all with respect to my transit authorities. In particular, in Orange County, we run a large bus system. We are getting ready for a streetcar. Obviously, California is working on this high-speed rail. I have a two-prong question. The first would be, any guidance that these agencies should follow in making these new systems, because we are developing, especially this fixed rail? Anything that we should worry about with respect to cyber attack? Second, the biggest issue that my transit agency has are all of this attack from a cyber perspective. Every day, every day, people are trying to get into their systems, they are trying to, you know, really raise chaos. What can they do, or what would you suggest?

Secretary JOHNSON. I would suggest that they work with our critical infrastructure protection experts within NPPD. The National Protection Programs Directorate, we have considerable expertise when it comes to rail security. TSA actually also has a rail security mission. But I have seen some fairly sophisticated analysis of how to build a secure rail station or a secure transit center that we can share with anyone who asks us.

Ms. SANCHEZ. Any of—OK. I will submit the rest of—more detailed questions along this topic, and hopefully, we can get some answers for the record, because they are very concerned about these cyber types of situations going on. Thank you. Thank you all.

Chairman MCCAUL. The Chair recognizes the gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Director Comey, first of all, thank you for your many years of service to our country. It is appreciated by many individuals.

I would like to ask you first about Syrian refugees. Before this committee last October, you testified that you had concerns about admitting Syrian refugees when a thorough background check was not possible; in fact, you called it a risk. Do you still have concerns about admitting Syrian refugees where you cannot conduct the thorough backgrounds, and do you consider them a risk now?

Mr. COMEY. Yes. Thank you, Mr. Smith. I think what all three of us said when we last talked about this together was we were comparing our ability to vet Iraqi refugees favorably with our ability to vet Syrian refugees. We have made great progress, and since we were last together, we have made even more progress at getting better at knowing what we know about anybody who is looking to come into the United States.

The point I was trying to make then and I still believe is true is that we will know, certainly on average, less about somebody

coming from Syria than somebody coming from Iraq, just given the United States' long-standing presence in Iraq.

So there is no such thing as zero risk. The challenge we face is not being able to see as rich a picture about somebody coming from Syria as from Iraq.

Mr. SMITH. Right.

Mr. COMEY. I have stayed away from the policy question about whether it is a good idea or bad idea to let in refugees. That is not for the FBI. So my view of it is basically the same as it was last October.

Mr. SMITH. OK. Because you said last October, there is risk associated with bringing anybody in from the outside, especially from a conflict zone like Syria, my concern there about bringing Syrian refugees into the United States is that there are certain gaps I don't want to talk about publicly in the data available to us.

So you stand by that statement——

Mr. COMEY. Yes.

Mr. SMITH [continuing]. There is a risk and you have concerns?

Mr. COMEY. Yes.

Mr. SMITH. OK. Thank you. Let me go to another subject. It doesn't have to do with terrorism, but it does have to do with National security. You testified before the Oversight Committee that former Secretary of State Clinton did not comply with the Federal Records Act, at least in some respects, and you were summarized as saying you thought she violated at least some aspects of the Federal Records Act.

Under the Federal Records Act, I understand that anyone found guilty of willfully and unlawfully concealing, removing, mutilating, obliterating, destroying, or attempting to do any such action against a Federal record can be fined and imprisoned for up to 3 years. In addition to fines and possible imprisonment, anyone holding Federal office who is convicted of this crime can lose his or her position and be disqualified from holding Federal office in the future.

If Mrs. Clinton violated the Federal Records Act, could these penalties apply to her?

Mr. COMEY. Mr. Smith, I do remember vividly my 4 hours and 40 minutes before the committee last week. I don't think I testified about that we had found a violation of the Federal Records Act. In fact, our investigation focused on Classified information, whether it was mishandled or transmitted in ways——

Mr. SMITH. Well, here is your exact statement. You were asked if you thought Secretary Clinton complied with the Department's policies under the Federal Records Act. Your first sentence back was: "I don't think so. At least in some respects, no." That was interpreted as your saying that she violated at least in part the Federal Records Act.

Mr. COMEY. Yes, I must—either I screwed that up or I was misunderstood. I thought I was answering a question about with respect to Department of State policy on their use of systems. I am no expert in the Federal Records Act, and that was not the gravamen of our investigation.

Mr. SMITH. Did you consider prosecuting her for violating the Federal Records Act?

Mr. COMEY. You said did I—did we consider that?

Mr. SMITH. Did you consider that?

Mr. COMEY. No.

Mr. SMITH. OK. Thank you, Mr. Comey.

Thank you, Mr. Chairman. Yield back.

Chairman MCCAUL. The Chair recognizes the gentleman from Rhode Island, Mr. Langevin.

[Microphone issues.]

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank you and the Ranking Member for holding this hearing. [Audio malfunction] testifying before.

Director Rasmussen, I was struck by your testimony that, speaking of degrading ISIL's capabilities and denying it access to fighters and resources, "clearly, progress has been made in these areas." Yet in your very next sentence you state, and I quote, "it is our judgment"—an example, "ISIL's ability to carry out terrorist attacks . . . abroad has not to date been significantly diminished."

So how do you square these two statements? Is it the result of the residual foreign fighters that traveled there before the flow was staunched? Is it more because of the home-grown violent extremist problem? Or is there some other explanation?

Mr. RASMUSSEN. Thank you for the question. I guess the way I would think about it is that we have always looked at ISIL as having multiple agendas, being a multifaceted organization. As we have talked about with this committee, they were in the business of trying to create and run a caliphate. As was in my testimony, I think we have made progress in diminishing some of their capacity to do that, shrinking the territory that they hold, denying them as rich a flow of resources as they had at the beginning of the conflict.

But they have also got another prong to their agenda, and that is this effort to carry out or inspire or enable attacks at various places around the globe. That line of effort that ISIL is engaged in, we have had less success at diminishing their capacity in that area. As I said, we shouldn't be surprised because there isn't necessarily a one-for-one connection between success in our efforts in one area—denying them territory, constraining their resources—and success in this other area—diminishing their attack capacity.

Is is obviously true that the greater success we have in shrinking their territory and as we shrink their resource picture, over time we will degrade their capacity. I was simply making the analytic observation that that may take time, and that not only is there a one-for-one correlation in progress across these two lines of effort, but there may be a significant lag as well.

Organizations have proven that even when they are relatively small, operating in a clandestine way, and not with all the benefits of a State or a caliphate, can still carry out or direct complex terrorist attacks around the globe. So that is simply the distinction we are trying to make, is that there are multiple things going on with ISIL.

Mr. LANGEVIN. Thank you.

So to the panel, as you all know, I am very deeply concerned about the issue of cybersecurity, something I have spent years on, and I share this with both the Chairman, as well as with the DNI,

who in his recent threats testimony has time [audio malfunction] the threat that we face in this domain.

So one of the frustrating aspects of cybersecurity, of course, for me and for many others, is the lack of reliable metrics. So for each of you, how do you measure how much the threat is increasing and what progress we are making in defending ourselves?

So for each of you, I would be interested to know what metrics you personally rely on to make these assessments. How do you decide whether we are moving forward, treading water, or falling behind?

Secretary JOHNSON. Congressman, the metrics that first come to mind for me in the DHS mission, we are building the capability right now in our Federal civilian .gov system to block intrusions into the system. So I measure the number of intrusions blocked. The last time I looked with E3A, Einstein 3A, we had blocked well in excess of 500,000 in the Federal civilian system.

I also measure our progress in cybersecurity by the number of private-sector entities, ISAOs, companies that we have signed up to share our automated information-sharing capability, and our progress in terms of getting Federal agencies on-line with our DHS capabilities.

So those are 3 ways right there. I defer to the other witnesses.

Mr. LANGEVIN. Thank you.

Director Comey.

Mr. COMEY. As you know, Congressman, it is an area that is not susceptible of a great set of metrics, but we look at essentially the demand for our services, complaints to our Internet Crime Complaint Center, the number of cases opened—that is, referrals to us from the private sector or other Government agencies—as a proxy for the threat that we face. There are other qualitative measures, but those are the two that come to mind.

Mr. RASMUSSEN. I have a somewhat narrower slice of this problem because I worry about it from the perspective of an international terrorist organization trying to develop a cyber capability. So there, the metrics I would look at is the amount of intelligence reporting we see over time that speaks to a terrorist organization's desire to gain that capability, to threaten the United States or other countries with that capability, and then also when they have been able to succeed at doing that.

Thus far, I think it is generally true that this has been something that terrorist organizations aspire to do, but thus far, without as much success as they would have liked.

Mr. LANGEVIN. Thank you.

I know my time has expired. I hope we can continue, though, to focus on this metric aspect so that we understand whether we are in fact making progress and not just rely on anecdotal evidence. But thank you for the work you are doing.

I yield back the balance of my time.

Chairman MCCAUL. The gentleman from South Carolina, Mr. Duncan, is recognized.

Mr. DUNCAN. Thank you, Mr. Chairman.

I would like to recommend to my colleagues that they view Senator Tim Scott's floor speech from yesterday. It is on his Facebook page. You can probably call his office to get a copy of it.

I would like to provide, when it gets here, a copy of that speech for the record, Mr. Chairman.

Chairman MCCAUL. Without objection, so ordered.

[The information follows:]

EXCERPT SUBMITTED FOR THE RECORD BY HON. JEFF DUNCAN

OUR AMERICAN FAMILY

Congressional Record S5055, July 13, 2016.

Mr. SCOTT. Mr. President, I rise today to give my second speech this week discussing the issues we are facing as a nation following last week's tragedies in Dallas, Minnesota, and Baton Rouge. This speech is perhaps the most difficult because it is the most personal.

On Monday, I talked about how the vast majority of our law enforcement officers have only two things in mind: protect and serve. But, as I noted then, we do have serious issues that must be resolved.

In many cities and towns across the Nation, there is a deep divide between the Black community and law enforcement. There is a trust gap, a tension that has been growing for decades. And as a family, one American family, we cannot ignore these issues because while so many officers do good—and as I said on Monday, we should be very thankful and supportive of all of those officers who do good—some simply do not. I have experienced it myself.

So today I want to speak about some of those issues—not with anger, although I have been angry. I tell my story not out of frustration, although at times I have been frustrated. I stand here before you today because I am seeking for all of us, the entire American family, to work together so we all experience the lyrics of a song that we can hear but not see: peace, love, and understanding. Because I shuddered when I heard Eric Garner say, "I can't breathe." I wept when I watched Walter Scott turn and run away and get shot in the back and killed. And I broke when I heard the 4-year-old daughter of Philando Castile's girlfriend tell her mother, "It's OK, I'm right here with you." These are people. Lost forever. Fathers, brothers, sons.

Some will say and maybe even scream: But they have criminal records. They were criminals. They had spent time in jail.

And while having a record should not sentence you to death, I say, OK, then, I will share with you some of my own experiences or the experiences of good friends and other professionals.

I can certainly remember the very first time I was pulled over by a police officer as just a youngster. I was driving a car that had an improper headlight. It didn't work right. And the cop came up to my car, hand on his gun, and said: Boy, don't you know your headlights are not working properly? I felt embarrassed, ashamed, and scared—very scared.

But instead of sharing experience after experience, I want to go to a time in my life as an elected official to share just a couple of stories as an elected official. But please remember that in the course of 1 year, I have been stopped seven times by law enforcement officers—not four, not five, not six, but seven times in 1 year as an elected official. Was I speeding sometimes? Sure. But the vast majority of the time I was pulled over for nothing more than driving a new car in the wrong neighborhood or some other reason just as trivial.

One of the times I remember I was leaving the mall. I took a left out of the mall, and as soon as I took a left, a police officer pulled in right behind me. That was my first time. I got to another traffic light, and I took another left into a neighborhood. The police followed behind me. I took a third left onto the street that at the time led to my apartment complex and then finally I took a fourth left coming into my apartment complex, and then the blue lights went on. The officer approached the car and said that I did not use my turn signal on the fourth turn. Keep in mind, as my colleagues might imagine, I was paying very close attention to the law enforcement officer who followed me on four turns. Do you really think that somehow I forgot to use my turn signal on the fourth turn? Well, according to him, I did.

Another time, I was following a friend of mine. We had just left working out and we were heading out to grab a bite to eat at about 4 o'clock in the afternoon. He pulls out, and I pull out right behind him. We are driving down the road, and the blue lights come on. The officer pulls me into the median, and he starts telling me that he thinks perhaps the car is stolen. Well, I started asking myself—because I was smart enough not to ask him but was asking myself—is the license plate com-

ing in as stolen? Does the license plate match the car? I was looking for some rational reason that may have prompted him to stop me on the side of the road.

I also think about the experiences of my brother, who became a command sergeant major in the U.S. Army, the highest rank for an enlisted soldier. He was driving from Texas to Charleston and was pulled over by a law enforcement officer who wanted to know if he had stolen the car he was driving because it was a Volvo.

I do not know many African-American men who do not have a very similar story to tell, no matter the profession, no matter their income, no matter their position in life.

I also recall the story of one of my former staffers—a great guy, about 30 years old—who drove a Chrysler 300, which is a nice car, without question, but not a Ferrari, not a super nice car. He was pulled over so many times here in DC for absolutely no reason other than that he was driving a nice car. He sold that car and bought a more obscure form of transportation. He was tired of being targeted. Imagine the frustration, the irritation, the sense of a loss of dignity that accompanies each of those stops.

Even here on Capitol Hill, where I have had the great privilege of serving the people of South Carolina as a U.S. Congress Member and as a U.S. Senator for the last 6 years—for those who don't know, there are a few ways to identify a Member of Congress or Senate. Well, typically, when you have been here for a couple of years, the law enforcement officers get to know your face and they identify you by face, but if that doesn't happen, then you have an ID badge, a license you can show them, or this really cool pin. I oftentimes said the House pin was larger because our egos are bigger. So we have a smaller pin in the Senate. It is easy to identify a U.S. Senator by our pin.

I recall walking into an office building just last year after being here for 5 years in the capital, and the officer looked at me, full of attitude, and said, "The pin I know, and you I don't. Show me your ID." I will tell you, I was thinking to myself, either he thinks I am committing a crime, impersonating a Member of Congress, or—or what? Well, I will tell you that later that evening I received a phone call from his supervisor apologizing for the behavior. That is at least the third phone call I have received from a supervisor or the Chief of Police since I have been in the Senate.

So while I thank God I have not endured bodily harm, I have felt the pressure applied by the scales of justice when they are slanted. I have felt the anger, the frustration, the sadness, and the humiliation that comes with feeling like you are being targeted for nothing more than being just yourself.

As the former staffer I mentioned earlier told me yesterday, there is absolutely nothing more frustrating, more damaging to your soul than when you know you are following the rules and you are being treated like you are not.

But make no mistake—no matter this turmoil, these issues should not lead anyone to any conclusion other than to abide by the laws. I think the Reverend Martin Luther King, Jr., said it so well. Returning violence with violence only leads to more violence and to even darker nights, nights, to paraphrase, without stars. There is never ever an acceptable reason to harm a member of our law enforcement community—ever. I don't want anybody to misinterpret the words I am saying.

Even in the times of great darkness, there is light. As I shared Monday, there are hundreds—thousands of stories of officers who go beyond the call of duty. Ms. Taylor—whom I spoke about on Monday night—at the Dallas incident was covered completely by at least three officers who were willing to lose their lives to save hers. We have a real opportunity to be grateful and thankful for our men and women in uniform.

I shared another story on Monday night as well, and while the one I want to tell you today does not involve a tragic loss of life, it does show support that meant a lot to me at the time it occurred. Prior to serving in the U.S. Senate, I was an elected official on the county level, State level, and a Member of the U.S. Congress. I believe it is my responsibility to hang out and be with my constituents as often as possible and to hear their concerns. At some point during my time as a public servant, I traveled to an event I was invited to along with two staffers and two law enforcement officers—all four were White, and me. When we arrived at the event, the organizer seemed to have a particular issue with me coming to the event. They allowed my two staffers to go into the event and seemed fine with allowing the two officers to go into the event, who both said they weren't going in unless I was going in. So in order to avoid a tense situation, I opted to leave because there is no winning that kind of debate ever. But I was so proud and thankful for those two law enforcement officers who were enraged by this treatment. It was such a moment that I will never forget and a situation that I would love to forget.

This situation happens all across the country. This situation happens all across the country whether or not we want to recognize it. It may not happen a thousand times a day, but it happens too many times a day, and to see it as I have had the chance to see it helps me understand why this issue has wounds that have not healed in a generation. It helps me to appreciate and to understand and helps me communicate why it is time for this American family to have a serious conversation about where we are, where we are going, and how to get there. We must find a way to fill these cracks in the very foundation of our country.

Tomorrow I will return with my final speech in this three-part series on solutions and how to get to where we need to go by talking about the policies that get us there and the people solutions because I, like you, Mr. President, don't believe that all answers are in government. I don't believe all the solutions we need start in government, but we need people doing things that only individuals can do.

Today, however, I simply ask you this: Recognize that just because you do not feel the pain, the anguish of another, does not mean it does not exist. To ignore their struggles—our struggles—does not make them disappear; it simply leaves you blind and the American family very vulnerable. Some search so hard to explain away justice that they are slowly wiping away who we are as a nation. We must come together to fulfill what we all know is possible here in America—peace, love and understanding. Fairness.

Thank you, Mr. President.

Mr. DUNCAN. Senator Scott talks about his experiences as an African American male and some of the things we are dealing with in this country. As a white man, I can't relate to that, so I need those experiences from Senator Scott and others. So I would encourage everyone to watch it, because I think it is important in the dialog that we are having.

The Ranking Member mentioned no fly, no buy, and asked the Secretary about that. The problem with that, it seems common sense, but the problem with that is no one can substantially tell us how someone gets on the no-fly list or, when it is adjudicated, how they get off the no-fly list with any complete understanding from Members of Congress, and we have asked.

Because especially on someone's suspicion that somebody might be involved in or future involved in an act of terror or crime, when we are talking about the Second Amendment, we need to realize that no fly, no buy also violates the Fifth and Sixth Amendment guarantees of due process. So how do you get on it? Do you have a chance to view the charge and interview the witnesses, hear testimony, defend yourself?

So we need to be cautious when we start delving into limiting our Second Amendment rights by also limiting our Fifth and Sixth Amendment rights.

Secretary Johnson mentioned in his opening statement, written and verbal, San Bernardino and Orlando. We also need to remember that ISIS and al-Qaeda, Islamic, radical Islamic jihad-inspired terrorism acts incurred at Fort Hood, Chattanooga, Little Rock, the beheading in Oklahoma, Boston Marathon, and there are others. Those are what I came across just off the top of my head. These were ISIL-inspired acts of terrorism here in the United States.

I don't believe that we can throw Charleston into the same mix. I believe that was a law enforcement issue. I don't believe that guy was inspired by any outside groups like ISIL in the realm of radical Islamic terrorism.

So the question I have for Secretary Johnson, and I get this in my district all the time, we use and the title of the hearing uses "ISIS," the Islamic State in Iraq and Syria, right? The administration uses "ISIL," and I fully understand the Islamic State in Iraq

and the Levant. Why? Why is that terminology used by the administration?

Secretary JOHNSON. I have used ISIL, I have used ISIS, I have used Islamic State, Secretary Kerry uses Daesh, the press uses different phrases. We generally refer it to as ISIL, but not exclusively. There is no hard and fast rule.

Mr. DUNCAN. OK.

Secretary JOHNSON. The Secretary of State uses a different word.

Mr. DUNCAN. The reason I ask that question is because since 2001 and since the 9/11 Commission Report came out, we have seen, especially under this administration, the disappearing language of terror, where words related to Islamic jihad have been stripped from the lexicons of DOD, of law enforcement here, and the Homeland Security Committee, we have had hearings where we have talked about the disappearing language of terror.

I believe, and many others in the intelligence community that I have talked to, many others in the defense industry say if you can't identify an enemy, it is very difficult to defeat the enemy. I want to make sure that we are talking about things in the right terms. If I am using the wrong term, I want to know. But I will say that what we see in this country with these acts in San Bernardino and Fort Hood is radical Islamic jihad, radical Islamic terrorism. So I want to make sure we talk about that.

Your Department was set up in 2003, 22 agencies combined, but when I go through the list of folks that are dealing with counterterrorism in this country, we have got the Department of State. We had a hearing yesterday in the Foreign Affairs Committee where the Department of State has the former Center for Strategic Counterterrorism Communications, now known as Global Engagement Center. They have got a couple other offices at the Department of State dealing with counterterrorism.

So we have got DOD fighting ISIS, and also with SOUTHCOM and AFRICOM, all dealing with elements of ISIS and al-Qaeda and other terrorism. NCTC, we have got the Director here. We have got JTTFs all over the country. We have got the National Targeting Center looking to make sure that our container shipping is safe.

Now we have got this at Department of State. We have got a lot of elements within the Department of Homeland Security looking at, whether it is ISIS in general, whether it is border security, whether it is the virtual sphere of *Dabiq* and *Inspire* and Twitter and Facebook and all that, we have got the dark web. So we have got all those multiple agencies trying to do the same mission.

Are we not too big? The 9/11 Commission Report pointed out the walls of separation between agencies and that information wasn't shared. That is the reason your agency was set up.

Help me assure the American people, Mr. Secretary, that because of all this, Department of State, your agency, and every element that I mentioned, that we are not creating another cumbersome large bureaucracy where we are not sharing information and that things might fall through the cracks. Help me assure the American people of that.

Secretary JOHNSON. Congressman, my top priority, since I have been Secretary, is management reform, removing the stovepipes just within the Department of Homeland Security. Through our

Unity of Effort initiative, I think we have come a long way in doing that.

Two thousand two was the largest realignment of our Government to create my Department since the creation of the Department of Defense. It is a work in progress, but I think that through a number of the reforms we have put in place since I have been Secretary, we have moved a long way in the right direction.

Speaking, I think, for all of us, I think we all do a much better job of connecting the dots, sharing information where we should. Every incident, every attack is a lesson learned from which we should draw lessons. But I think we are moving in the right direction. I think we have come a long way, sir.

Mr. DUNCAN. Thank you for that. This committee was set up to oversee you and your agency so that those walls will come down and we don't miss signals.

Mr. Chairman, thanks for the leniency, and I yield back.

Chairman MCCAUL. The Chair recognizes the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman and the Ranking Member, thank you so very much for this hearing and the combination of outstanding Americans who serve this Nation.

Let me thank all of you for your service.

I will not predict, Secretary Johnson, that this is your last moment to testify in this committee, but I will say to you, thank you for your service. You may be going on and on and on, we do not know, but we thank you for your service.

We live in difficult times, and I believe that we should be a partner with you. Even as we have the stovepipes of the three branches of Government, I take the responsibilities of the Homeland Security Department, the Department of Justice, FBI, Mr. Rasmussen, your work, very seriously.

Because we have used the name Homeland Security so often, I have my own nightmares that as things proceed, the Nation will look to the Homeland Security, to the elements of Justice, and ask the question why. I would like to be able to at least answer that we did everything that we could probably do.

Let me start with you, Mr. Director, and let me ask the Chairman to ask unanimous consent to put into the record "Strengthening the Federal Cybersecurity Workforce."

Chairman MCCAUL. Without objection, so ordered.

[The information follows:]

STRENGTHENING THE FEDERAL CYBERSECURITY WORKFORCE

July 12, 2016, Shaun Donovan, Beth Cobert, Michael Daniel, Tony Scott

Summary: As directed by the Cybersecurity National Action Plan and 2017 Budget, today we are releasing the first-ever Federal Cybersecurity Workforce Strategy.

Today the Administration is directing a series of actions to identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service and for our Nation.

Every day, Federal departments and agencies face sophisticated and persistent cyber threats that pose strategic, economic, and security challenges to our Nation. Addressing these cyber threats has required a bold reassessment of the way we approach security in the digital age and a significant investment in critical security tools and our cybersecurity workforce. And these threats demand that we continue to enhance the security of the Federal digital infrastructure and improve the ability to detect and respond to cyber incidents as they occur. That is why, in 2009, President Obama initiated a comprehensive strategy to confront this ever-evolving chal-

lenge. The strategy brings all levels of government together with private industry, academia, international partners, and the public, to raise the level of cybersecurity in both the public and private sectors; deter and disrupt adversary activities in cyber space; improve capabilities for incident response and resilience; and enact legislation to both incentivize and remove legal barriers to cybersecurity threat information-sharing among private entities and between the private sector and the Government. While we have made significant progress, we must do more.

THE CHALLENGE

The Federal cybersecurity workforce has the exciting and challenging mission of protecting government information technology (IT) systems, networks, and data from sophisticated adversaries; safeguarding sensitive data; supporting our Nation's financial, energy, health care, transportation, and other critical systems; and securing our critical infrastructure and intelligence systems. However, the supply of cybersecurity talent to meet the increasing demand of the Federal Government is simply not sufficient. As part of a broad-sweeping review of Federal cybersecurity policies, plans, and procedures, the Cybersecurity Sprint launched by the Office of Management and Budget last year revealed two key observations about the Federal cybersecurity workforce:

Federal agencies' lack of cybersecurity and IT talent is a major resource constraint that impacts their ability to protect information and assets; and,

A number of existing Federal initiatives address this challenge, but implementation and awareness of these programs are inconsistent.

Moreover, this shortfall affects not only the Federal Government, but the private sector as well. Recent industry reports project this shortfall will expand rapidly over the coming years unless private-sector companies and the Federal Government act to expand the cybersecurity workforce pipeline to meet the increasing demand.

THE OPPORTUNITY

To address these and other cybersecurity challenges, earlier this year the President directed his Administration to implement the Cybersecurity National Action Plan (CNAP)—a capstone of more than 7 years of determined effort—which takes near-term actions and puts in place a long-term strategy that builds on other cybersecurity efforts while calling for innovation and investments in cybersecurity education and training to strengthen the cybersecurity talent pipeline. As directed by the CNAP and the President's 2017 budget, today we are releasing the first-ever Federal Cybersecurity Workforce Strategy to grow the pipeline of highly-skilled cybersecurity talent entering Federal service, and retain and better invest in the talent already in public service. And it sets forth a vision where private-sector cybersecurity leaders would see a tour of duty in Federal service as an essential stop in their career arc.

The Strategy establishes four key initiatives:

- *Expand the Cybersecurity Workforce through Education and Training*.—The Cybersecurity Workforce Strategy supports the CNAP initiatives that propose investing $62 million in Fiscal Year (FY) 2017 funding to expand cybersecurity education across the Nation. This funding will lay the foundation needed to ultimately address the shortage of cybersecurity talent across the country. These initiatives include offering competitive scholarships and covering full tuition for college and university students through the CyberCorps®: Scholarship for Service program; collaborating with academic institutions to develop guidance for cybersecurity core curriculum and allow colleges and universities to expand their course offerings; and providing program development grants to academic institutions to hire or retain professors, adopt a cybersecurity core curriculum and strengthen their overall cybersecurity education programs.
- *Recruit the Nation's Best Cyber Talent for Federal Service*.—The Workforce Strategy initiates efforts to implement a Government-wide recruitment strategy that includes enhanced outreach efforts to diverse cyber talent—including women, minorities, and veterans—from apprenticeship programs, colleges, universities, and private industry, as part of a comprehensive plan. Over the coming months we will partner with agencies to find ways to streamline hiring practices consistent with current statutes and leverage existing hiring authorities, as appropriate, to quickly bring on new talent. We will explore opportunities to establish a cybersecurity cadre within the Presidential Management Fellows program that leverages the recent success of the Presidential Innovation Fellows program and other dynamic approaches for bringing top technologists and innovators into Government service. Additionally, we will explore opportu-

nities to expand the use of new or revised pay authorities that can serve as a model for future Government-wide efforts.

- *Retain and Develop Highly-Skilled Talent*.—To improve employee retention and development efforts, the U.S. Office of Personnel Management (OPM) will work with Federal agencies to develop cybersecurity career paths, badging and credentialing programs, rotational assignments, and foster opportunities for employees to obtain new skills and become subject-matter experts in their field. Additionally, the Workforce Strategy directs the development of a Government-wide cybersecurity orientation program for new cybersecurity professionals to improve information sharing and employees' knowledge of upcoming developmental and training opportunities. The Workforce Strategy also looks to increase the use of special pay authorities, and improve training and development opportunities for cyber and non-cyber employees.
- *Identify Cybersecurity Workforce Needs*.—Cybersecurity is a dynamic and cross-cutting field, and effective workforce planning requires a clear understanding of the gaps between the workforce of today and the needs of tomorrow. The Workforce Strategy directs agencies to adopt a new approach to identifying their cybersecurity workforce gaps by using the National Cybersecurity Workforce Framework developed by National Initiative for Cybersecurity Education (NICE) partner agencies, which identifies 31 discrete specialty areas within cybersecurity workforce. Agencies are now able to better identify, recruit, assess, and hire the best candidates with specific cyber-related skills and abilities, and we are already making progress in this effort. The Federal Government has already hired 3,000 new cybersecurity and IT professionals in the first 6 months of this fiscal year. However, there is clearly more work to do, and we are committed to a plan by which agencies would hire 3,500 more individuals to fill critical cybersecurity and IT positions by January 2017.

Cybersecurity is a shared responsibility among agency leadership, employees, contractors, private industry, and the American people. And the Workforce Strategy details numerous initiatives to harness this collective power and help strengthen the security of Federal networks, systems, and assets. To address cybersecurity challenges in the immediate future, the administration will invest in the existing Federal workforce through initiatives focused on training and retaining existing talent. At the same time, the Government will adjust the way it recruits, including the way it approaches talented students and potential employees in the cybersecurity workforce outside Federal service.

We must recognize that these changes will take time to implement, and the Workforce Strategy's long-term success will depend on the attention, innovation, and resources from all levels of government. The initiatives discussed in this Strategy represent a meaningful first step toward engaging Federal and non-Federal stakeholders and provide the resources necessary to establish, strengthen, and grow a pipeline of cybersecurity talent well into the future.

Shaun Donovan is the Director of the Office of Management and Budget.
Beth Cobert is the Acting Director of the U.S. Office of Personnel Management.
Michael Daniel is Special Assistant to the President and Cybersecurity Coordinator.
Tony Scott is the U.S. Chief Information Officer.

Ms. JACKSON LEE. Thank you.

In a speech on the 26th, Mr. Comey, before the Conference on Cyber Engagement, you indicated in terms of threats in the cyber world, there were 5 groups. That includes China, Russia, Iran, nations, North Korea, and then multinational cyber syndicates that deal with selling cyber information to the highest bidder. You then mentioned individuals who were purveyors of ransomware, then hacktivists, which we all contend with, and terrorists.

Would you care to offer pointedly which of those gives you the greatest pain and what would you call on Congress to do about it in being a partner in this effort?

Mr. COMEY. I think the biggest concern are the top of that stack of badness, which are the nation-States and the near nation-State actors who are engaged in sophisticated computer intrusion aimed at our National security. That is a very, very important part of the FBI's life. Maybe tied, because of the impact on ordinary citizens, are the criminals that are using the internet to lock up people's

systems, to extort money from them, to threaten their children. That is computer-enabled crime.

So the biggest intrusion problem is the nation-States. The biggest computer-enabled crime problem are the variety of thugs and fraudsters and criminals who are coming at us that way.

I think Congress has been very supportive of the Department of Homeland Security and the FBI, prodding us to work better together, to share information better with the private sector, which is the answer, and giving us the tools and the rules of the road to assure the private sector that you not only need to share stuff with us, we will all be safer if you do.

Ms. JACKSON LEE. Well, let me thank you for that. I am going to get around to that again, but I want to answer Mr. Duncan's question.

First of all, I did see Tim Scott's very eloquent speech and thank him for his life experience. But I introduced the No Fly for Foreign Terrorists, and it answers Mr. Duncan's questions in terms of looking on the TSDB and making sure that past weaknesses have been addressed, asking the GAO to do that, and the extent to which existing vulnerabilities may be resolved or mitigated, making sure that you have a clean data list to be able to utilize. I hope that bill, it has passed at the House, will get to the Senate, and we will have at least a guideline to deal with.

But I want to pursue the idea of cybersecurity from the perspective of another bill I have, H.R. 85, that says that we need a stronger relationship between the Government cyber system and the private sector cyber system, and also to have a back-up when either of us are deemed either vulnerable or incapacitated.

Mr. Comey, what do you see in those alignments in making sure that we are secure from the private sector and the Federal sector based upon the breaches that we have had, FBI has been impacted, Department of Homeland Security has been impacted, the Office of Personnel has been impacted?

Mr. Comey.

Mr. COMEY. I think we are making great progress. It is not good enough. It is nowhere near good enough yet. I think we are getting reports of somewhere in the area of 20 percent of the incidents actually happening. We have got to do better than that.

I think businesses are starting to figure out that it is an imperative, a business imperative to work better with the Government, and I think the Sony hack sent that message in a great way to boards and to CEOs. So I would give it an interim grade of OK.

Ms. JACKSON LEE. May I ask these questions to Mr. Johnson and Mr. Rasmussen?

Secretary Johnson, I have seen your work on countering violent terrorism. I have been engaged with the Muslim community very extensively and have them tell me how frightened they are now, and I have tried to say how much we are with you but how important it is to be part of this team. I would like you to share your thoughts about how that works.

Mr. Rasmussen, let me throw you sort-of a curve ball of sorts and ask you about something called—because you deal collectively with police and you work on terrorism issues. I want to associate myself with Mr. Thompson. I think the individual—and my sympathy to

my fellow Texans, the loss of those officers. I was at the memorial. But I do think that was a terrorist act. It was an individual intending to terrorize, it might have been hate, racial hate, using a weapon of war.

There are a number of things happening. I bring to your attention swatting, which may wind up causing an enormous tragedy, that is being a manipulation of emails and breaching, and I just hold up, this is what is happening to people around the Nation. I think I am a victim of such from a person in Bangladesh that is happening to me personally in my home in Houston. I didn't understand what it was, but it is a dangerous phenomenon.

So I am wondering whether or not that is to the attention of the National terrorism research and what you think we can do about it.

Mr. Johnson.

Secretary JOHNSON. Well, very quickly, ma'am, we need to continue to go to these communities. I have been to Houston. I have been to a lot of other communities. As we approach these communities, we have to remember that they are not a monolith. Islam is as diverse as Christianity. A Somali American community in Minneapolis looks very different from a Syrian American community in Houston. We encounter a fair amount of suspicion, as you have noted, when the Federal Government goes to these communities, but I think we have to keep at it and keep building bridges.

Ms. JACKSON LEE. Mr. Rasmussen.

Mr. RASMUSSEN. Thank you for bringing this to my attention as well. We clearly are seeing an increase in the degree to which foreign terrorist organizations are using on-line technology in order to try to intimidate people, in order to try to put out target lists, to try to inspire individuals to go after law enforcement, intelligence officials, military personnel, et cetera.

But at the same time there is also a great deal of focus in the criminal world on this capability, as well, and people trying to use the same capability to intimidate or to pursue some criminal end, as well.

So what we try to do is discern as best we can the motivation between the act. If it ends up being something tied to a terrorist, a terrorist group, or a terrorist motivation, we approach it in a certain way, and it becomes much more of a law enforcement matter if it can be pursued as a criminal act. But it is something we are seeing much more frequently and something we are devoting a lot of work to trying and understand.

Ms. JACKSON LEE. Thank you.

Mr. Chairman, may I just put another item in the record, "Cybersecurity and Crypto on the Internet."

Chairman MCCAUL. Without ojection, so ordered.*

Ms. JACKSON LEE. Thank you.

Chairman MCCAUL. We have votes at 12:20. We have several Members left that would like to ask questions. I am going to try to limit everybody to 5 minutes from this point forward, if the gentlelady has completed her questions.

---

*H.R. 85 is available at *https://www.congress.gov/114/bills/hr85/BILLS-114hr85ih.pdf* and has been retained in committee files.

Ms. JACKSON LEE. I didn't have anything else.

Chairman MCCAUL. In deference to other Members.

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

Chairman MCCAUL. I appreciate that. Without objection, that is entered into the record.

The Chair now recognizes Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman.

In November, December 2015, a report surfaced of ISIS and affiliated groups making and using fake travel documents to gain access to Western Europe and beyond.

Is ISIS still producing and making use of these forged travel documents, Secretary Johnson?

Secretary JOHNSON. It is a general concern. I am not sure how much more we can get into that in a public setting. Perhaps Nick could have more to say in a public setting. I am not sure how much more, though.

Mr. RASMUSSEN. I think I would probably leave it there too. It is something we certainly have seen ISIL and other terrorist organizations looking to develop and use that capability. We are doing our best to understand that, the way they are using it, so that we can either advise our European partners, who face this in a much more frontline way than we do, but also to inform our own ability to detect false documentation at the border.

Secretary JOHNSON. Congressman, I should add that within DHS we have a very sophisticated fraudulent detection capability when it comes to identification documents, travel documents. It is getting better all the time.

Mr. WALKER. Director Comey, around this same time late last year, *Politico* and AP reported that ISIS was taking advantage of the refugee crisis by providing forged travel documents to desperate individuals fleeing war and profiting from the practice.

In addition to the profit motive, has the FBI seen evidence that ISIS is providing these documents to their own fighters for attacks abroad?

Mr. COMEY. Well, we certainly saw it in the case of the attacks in Paris and Brussels. I agree with what my colleague said, we know it is a part of ISIL's tradecraft. By the way, I think the name ISIL actually better captures the danger and the aspiration of this group of savages than ISIS does, because it is bigger than just Syria. But I would just echo what my colleagues said.

Mr. WALKER. As part of the United States' response to this threat late last year, we demanded action from 5 different European States and threatened to remove them from the Visa Waiver Program if no action was taken. What has the response been of those States, and what further steps have we taken to ensure our allies in Europe are vetting travel documents properly?

Secretary JOHNSON. Congressman, I would have to know the 5 specifically. We have, late last year, insisted on the use of e-Passports. We have insisted on the use of Federal air marshals on flights to the United States. We have insisted on better use of API/PNR data, that is travel data. We have, in general, sought what we refer to as HSPD–6s from these countries, Homeland Security Presidential Directive 6s, that guarantee security both within these countries in terms of the travel and travel to the United States,

using the Visa Waiver Program as the entree into asking for those things.

Mr. WALKER. OK. What actions, Director Comey, has the FBI taken to independently identify and prevent travelers from using their forged documents?

Mr. COMEY. Well, obviously, working very, very closely with our colleagues at DHS, especially CBP, and, most importantly, our colleagues outside the United States to put in place tripwires so they share with us any intel they get that they may be looking to use a particular channel or particular type of document. So the most important thing we can do is remain knitted closely together.

Mr. WALKER. Secretary Johnson, do you have anything to add to that?

Secretary JOHNSON. Yes. As I mentioned earlier, we have a fraudulent detection capability when it comes to travel documents. We are very concerned about fraudulent passports, fraudulent travel documents. As you noted, we have seen that in Europe.

I should note that to travel to this country visa-free, you have to be a citizen of that country, in Europe, for example. But this is something we have been focused on it and it is something we are concerned about, sir.

Mr. WALKER. In wrapping up, let me pass along my compliments to Director Comey for the good testimony in another hearing the other day.

I was impressed that for 4 hours and 40 minutes that you sat there without really any breaks.

Secretary Johnson, I haven't seen the latest report. I don't know how many States are left to file on the ballot, I don't know where you are headed, but whatever it is, I wish you the best. So thank you.

Chairman MCCAUL. The gentlelady from California, Mrs. Torres, is recognized.

Mrs. TORRES. Thank you, Mr. Chairman.

Thank you to the three of you for being here and for the on-going outreach that you are doing in my community. Certainly the Middle Eastern community that resides within the 35th Congressional District truly appreciates the fact that you have made an effort to come out and help them through some very difficult times after the San Bernardino incident.

I want to talk a little bit about the CVE grant. I want to get a better idea as to who qualifies and specifics of that grant. How is it going to be awarded? Are you looking at communities with populations of at-risk youth, young communities, big cities, small cities, types of population? What are the criteria that you are using for these grants?

Secretary JOHNSON. Congresswoman, there is a 32-page notice of funding opportunity that went out last week for the $10 million that Congress made available to us this year. We are hoping that Congress continues to fund our CVE efforts.

The opportunities center around basically developing resilience, challenging the narrative—that is, ISIL's narrative—training and engagement, managing intervention activities, and building capacity. Those are the broad parameters. They are more specifically set

forth in this 32-page document, which I am happy to provide to you.

Mrs. TORRES. Would home-grown violent extremist people, would those targets fall under that grant, communities that could have a potential of these types of——

Secretary JOHNSON. In general, yes, through intervention activities, through countermessaging. Countermessaging is not necessarily a Government mission.

Mrs. TORRES. Right.

Secretary JOHNSON. Because it wouldn't be credible if it were, me or the FBI. Through basic resources to encourage people to move in a different direction. Broadly speaking, that is the intent of this, but it is more specifically spelled out in this circular.

Mrs. TORRES. Other than law enforcement agencies, who else is your Department coordinating with? For example, Department of Education. Are there other resources where you are acquiring data to ensure that we are maximizing this grant with other potential grants that could be available to be utilized in these communities?

Secretary JOHNSON. Well, obviously, the grantees, those who apply for this funding are in a position to help. We will vet them carefully. We will make our grant awards carefully. So it is not just a law enforcement, homeland security mission. There are private local organizations that are in a position to help and I think that want to help.

Mrs. TORRES. On the issue of lone-wolf attacks that we have seen most recently, including law enforcement, there has been an increase in the number of threats against law enforcement personnel. In lieu of the two conventions coming up, how are you ensuring that the law enforcement community is prepared to deal with not just threats against the potential attendees, but threats against their own personnel that would be easy targets, easily identified?

Secretary JOHNSON. We intend to have within Homeland Security some 3,000 of our personnel dedicated to the security of each convention. I am quite sure that the security of our own personnel is a priority for our component heads. I am quite sure that among State and local law enforcement, they too are concerned about threats directed against law enforcement. But I think the average law enforcement officer would be the first one to say that their primary obligation is the protection of the people they serve.

Mrs. TORRES. But they have to deal also with open carry in one of those cities, and that includes long guns and automatic weapons, correct?

Secretary JOHNSON. Correct, yes. That is correct. Ohio, as I understand it, is an open-carry State.

Mrs. TORRES. Right.

Secretary JOHNSON. So that obviously is something that someone under State law and I suspect the Second Amendment has a right to do. But it does present a challenging situation, very plainly.

Mrs. TORRES. Thank you. I yield back.

Chairman MCCAUL. The Chair recognizes Mr. Carter.

Mr. CARTER. Thank you, Mr. Chairman.

Thank all three of you for being here. We appreciate your attendance today.

First of all, Director Comey, good to see you again. I saw you last week. Glad to have you back.

I want to talk briefly about the Orlando situation and about the terrorist attack, obviously, that happened there, and I want to talk to you about it in relation to Secretary Johnson.

My concern is communication. I am real big on communication. My question is this: What communication did the two of you have during that time? During the time that it was happening and immediately after it happened, was there any communication? What kind of communication takes place between all three agencies?

Mr. COMEY. Well, that last part of your question is the most important. It is vital that the people doing the actual work in our organizations talk to each other constantly, and they do because they are sitting together. The Joint Terrorism Task Force in Orlando, in all of our other cities is composed of some folks from Jeh's organization and mine. I don't remember exactly. I think the two of us actually hosted a Nation-wide call for all law enforcement in the wake of that.

Mr. CARTER. But certainly you communicated before that call?

Mr. COMEY. You know, I can't remember. I talk to Jeh quite frequently. It is possible I did. But I know for sure that we hosted—I think you were there, or you might have been on a SVTC someplace—we hosted a conference call for all law enforcement.

But the most important thing, he and I know each other very well, talk to each other all the time. That is great. But it is very, very much more important that our people work together seamlessly. That is the progress we have made in the last 15 years.

Mr. CARTER. You feel like that has worked well? You feel like there has been progress?

Secretary Johnson.

Mr. COMEY. I do.

Secretary JOHNSON. I do, sir. I do. Jim and I are together a lot, either in the Situation Room, at FBI headquarters, and the like. There have been instances where I will pick up a piece of intelligence that I am concerned about, and I will just literally pick up my Classified phone and call him to say: Hey, I want to be sure that you saw what I just saw.

So the level of communication at the senior-most levels, I have my under secretary for intelligence and analysis right here behind me, Frank Taylor, who works with the FBI all the time, literally, on these types of threats.

Mr. CARTER. OK. Let's talk about Omar Mateen specifically. It is my understanding that there are over 1,000 open investigations into home-grown extremists right now. When did you first learn about Omar Mateen? When was the first time you learned about that?

Mr. COMEY. The Orlando killer first came to our attention in the spring of 2013 when coworkers at the St. Lucie courthouse reported to the FBI that he was making concerning statements, and that is when we opened the preliminary investigation.

Mr. CARTER. Secretary Johnson, when?

Secretary JOHNSON. I am quite sure that while the FBI investigation was open, our personnel at the JTF were aware of the open investigation and aware of the identity of the individual. I

noted also that while the investigation was open, he was on a TSA selectee list as well. So our departments were clearly coordinating and sharing that information.

Mr. CARTER. OK.

First of all, all three of you appear to be fine gentlemen who truly want to protect our country, and we appreciate that.

Director Comey, let me ask you, you defended the investigations into the Orlando killer—and thank you for correcting me on that—and I believe you said that there was no indication that agents missed clues that could have prevented this massacre. Is that correct?

Mr. COMEY. That is correct. I said that immediately after, after going through the case file. I couldn't see, actually still don't see, anything that they didn't do they should have done.

But I have commissioned a lookback, a detailed scrub on it, which we do in all significant matters, by experienced people to come and say: Well, actually we should do this differently or that differently. I haven't gotten that report yet, and as I said at the time, I will be transparent when I get that report. But so far, I don't see anything.

Mr. CARTER. Was there any information, Mr. Secretary, that you think that Homeland could have helped with there?

Secretary JOHNSON. Based on what I know, Congressman, I am not in a position to second-guess those involved in the investigation. I am quite sure that Jim's lookback will be thorough, and he will be open and honest and transparent about any lessons learned that I may be able to benefit from within our Department too.

Mr. CARTER. I appreciate you saying that, and we are going to hold you at that. We need to learn from this.

Look, it is tough, and I know you have got a tough job, and it us going to take communication, cooperation. We are all in this together. I know that you gentlemen care about our country and you want to protect us. We have got to communicate. We have got to share information.

You know, I am just one of those who believes, if somebody gets upset, they get upset, they will get over it. But we need to communicate.

Thank you for your service.

Mr. Chairman, I yield.

Mr. RATCLIFFE [presiding]. The gentleman yields back.

The Chair recognizes the gentleman from Massachusetts, Mr. Keating, for 5 minutes.

Mr. KEATING. Thank you, Mr. Chairman. I have quite specific questions I will submit in writing.

But this has been a pretty tough few weeks for our country; tougher for the families that lost loved ones. When I was a DA before this job, I was in charge of enforcing civil rights laws in my jurisdiction, and I tried preventative initiatives, some of them successful, I believe, and I enforced the law. I enforced it against civilians and I enforced it against law enforcement when there were violations.

I also come from a police family. My dad, my brother, my niece either were or are police officers, and I understand that apprehension that families have as well.

You know, we have spent today talking about terrorist threats, and we talked about cyber, our response capabilities, our intelligence gathering. But I think our fundamental strength as a country is who we are as a country, that we have central tenets on respecting diversity and respecting the rule of law. The polls that we are seeing now are showing that our country is more divided than it has been in decades, and this is a concern, I think, that all of us share.

But if you could, it is the only thing I am going to ask you to reflect upon, but how important is it, for many reasons, but also for today's subject matter, to combat threats from inside and from outside? How important is it that we come together as a country?

I want to commend you for the statements that you have made during these trying times. I think you set great examples. But how important is it when we talk about these threats that we are together as a country? Can you take a few minutes, I will give the rest of my time, to just reflect on some of things we could do?

Secretary JOHNSON. Let me begin by saying that there are some awful loud voices on both ends of this debate, and I believe that the great majority of the American people, first of all, respect the role of law enforcement, recognize that the police officer is there to protect and to serve the community.

I also believe that most people recognize that the shooter in Dallas is not representative of the broader movement to see change in certain law enforcement practices.

I think that the key in the environment we are in is effective community policing. I see it work in my own community in Washington, DC, extraordinarily well.

So my hope is that in this period we redouble our efforts for law enforcement to engage the community—and I consider myself part of law enforcement—to engage the community, and let's all see the temperature go down a bit.

Mr. COMEY. We need each other. Whether it is to effectively stop terrorists or stop thugs or make neighborhoods safe, we need each other.

I have longed believed it is hard to hate up close. The answer is we have to get close to each other. We have to let people see the true heart of law enforcement, what we are really like. We are flawed because we are human, but we care deeply about the same things that the people we serve and protect do.

We have to make sure in law enforcement we see the heart of the people that we are serving and protecting and how they might see the world differently than we do.

It is hard to hate up close. It is easy to characterize groups. President Bush said something at the memorial service where I sat behind the Congresswoman, said: We tend to judge others by their worst moments and ourselves by our best intentions.

We have to stop that and we have to try to see the true heart of people across the divide, because there shouldn't be a divide, because our values are the same.

Mr. RASMUSSEN. I will just add one thing from a terrorism perspective. The people who work in all of our organizations who focus on counterterrorism spend every waking hour trying to prevent terrorist attacks from happening both at home and overseas. We have

zero tolerance among ourselves for failure in that regard. Nobody thinks anything is acceptable in that regard.

But failing that, if we fail, if somehow terrorist attacks happen, what we strive to create and foster is a sense of resilience so that the terrorist objective is not met even if the attack happens, even if we do suffer from terrorism.

It is a lot easier to be resilient if we are united. It is much easier to fly off in the aftermath of a terrorist attack if we are not united and to undermine that sense of resilience. Some societies, some countries seem to be more able to achieve that level of collective resilience than perhaps we have been.

Mr. KEATING. Thank you. It is harder to hate up close, and it is easier to be strong up close.

Thank you. I yield back.

Mr. RATCLIFFE. The gentleman yields back.

The Chair recognizes the gentlelady from Arizona, Ms. McSally, for 5 minutes.

Ms. MCSALLY. Thank you, Mr. Chairman.

Director Comey, I served in the Air Force to 26 years. I have had the highest level of security clearances and have been responsible for managing Classified information at many levels. As you know, we take handling of Classified information very seriously in the military, especially SCI and special access program information.

During your press conference, you stated, quote, "To be clear, this is not to suggest that in similar circumstances a person who engaged in this activity would face no consequences. And further, to the contrary, those individuals are often subject to security or administrative actions."

If an airman in the Air Force had conducted behavior similar to Secretary Clinton's, I am confident, at a minimum, they would lose their clearance, they would be kicked out, they would never get a clearance or be able to work for another Federal department or agency, in addition to other fines or anything else.

If someone were kicked out of the military for behavior similar to Secretary Clinton and applied for a job at the FBI under your leadership, would they be hired?

Mr. COMEY. I don't think I can answer that in the abstract. It would be a significant feature of a suitability review, though.

Ms. MCSALLY. Would they even get an interview if they have had a security violation to the nature of what Secretary Clinton did?

Mr. COMEY. I can't answer that as a hypothetical. It would be a significant feature. I can't say whether they wouldn't get an interview or not.

Ms. MCSALLY. OK. If someone were dismissed from the State Department for similar behavior, you are going to give me the same answer, you have to look at their circumstances?

Mr. COMEY. Yes. But again, there would be—there is a process. You know it in the military. There is a robust process, I can speak inside the FBI, to assess suitability and then to assess and adjudicate security violations among current employees.

Ms. MCSALLY. OK. Within the FBI, under your leadership, let's say your chief of staff or your deputy director mishandled Classified information in the same way that you know about, what would

be the security and administrative consequences that you would put upon them?

Mr. COMEY. Well, it would go through the regular review process that we have and it would be adjudicated. I don't want to, again, answer in hypothetical because we have to do this all the time. I don't want to prejudge any cases. But it would be looked at. It would be a significant security review. They could be fired, a sliding scale, all the way up to reprimanded, or lose pay, or there would be a series of disciplinary options for the board.

Ms. MCSALLY. You know more details about this case than anything. So now you are done with the criminal, and now you are looking at the administrative, what would you do?

Mr. COMEY. I am not prepared to say, because I think that gets me in an area of answering hypotheticals that could affect my own security review process. It would be a significant feature of a suitability and security review.

Ms. MCSALLY. So fines, losing their clearance, losing their job, what is on the menu?

Mr. COMEY. The most severe would be losing your job. Being walked out that day is probably the most serious. The least serious would be a reprimand of some sort. Then a sliding scale in between. People can get suspended. They can lose clearances. They can have clearances knocked down. There is a range of options.

Ms. MCSALLY. OK. I want to move on to physically how the Classified information got on an Unclassified system. You know, just in the military we have JWICS, SIPRNet, NIPRNet. You cannot cross those over in any way unless you either type in new information on the Unclassified, because you can't send an email from Classified to Unclassified. I am sure it is the same in the State Department.

So you either need to type a new email with the markings on it, right, those that were marked Classified, which you said there were three, or you need to, I guess, print or scan, or the most disturbing would be using a transferable media device, like a thumb drive, to get onto the secure system and move things over to the unsecure system, which could breach our entire security system, as you know. That is why they are banned in the military.

How, from your investigation, how did this Classified information get moved over out of those three options?

Mr. COMEY. Almost none of it involves information that was moved. Instead it involves email conversations about topics that are Classified.

Ms. MCSALLY. But if there is markings, you either are making a marking on an Unclassified system of a Classified nature, which is disturbing in and of itself, or you are physically moving it electronically.

Mr. COMEY. Right. There were three emails that bore portion markings on a paragraph, not header markings or footer markers, for "C," to indicate confidential. That was put on well down a chain, deeper and much lower level in the State Department. As I sit here, I don't know for sure, I think we concluded that somebody had typed a talking point for the Secretary way down the chain and marked that portion with a "C."

So it wasn't an uplift or a transfer. It was, as you said, a typing in the first instance and then putting a portion marking on it. But to be clear, it was just the portion that was marked, not the document.

Ms. MCSALLY. But still, on the Unclassified system, they are allowed to be transmitting Confidential information?

Mr. COMEY. No, because Confidential information is Classified information.

Ms. MCSALLY. Right.

Mr. COMEY. Top Secret, Secret, Confidential.

Ms. MCSALLY. Exactly. So they had to have actually typed "Confidential" on an email chain or they used transferable media.

Mr. COMEY. We have no indication of transferable media. What we think happened is someone typed a talking point on an unclassed system and then, for reasons that don't make any sense to you and to me——

Ms. MCSALLY. Right.

Mr. COMEY [continuing]. Marked it with a "C" to indicate that portion was Classified at the Confidential level.

Ms. MCSALLY. OK. Director Comey, I am sure you realize that those of us who have been involved in the security field, like you, I mean, this is concerning on many levels that I think needs a lot of follow-up for how that actually happened and what is going to happen to the individuals that actually did that.

Because if you are actually typing Classified information and markings on an Unclassified email, I mean, that is a security violation and those people should be held accountable as well.

Thank you, Director.

Thank you, Mr. Chairman. I yield back.

Chairman MCCAUL [presiding]. The Chair recognizes Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Chair.

I want to thank the three of you very much for the information you shared with us and that you come every time we ask. It has been very illuminating, the discussion we have had, and it has raised some questions that I would like to share with you.

No. 1, I wanted to talk to you, Secretary Johnson, you mentioned some grants that are available. I live in a district that is not part of the targeted area, the UASI area or things of that nature, but I live in an area that has a tremendous diversity of religious worshippers. Some of them have been asking us for assistance in grants that would help them to put things that would make them safer, be it cameras or whatever.

Would the grants that are being offered now, available, would any of them qualify, even though they are not in the target areas?

Secretary JOHNSON. Yes. There are grants for which a large number of religious institutions can take advantage of for homeland security. Sitting here, I can't recall the name of the grant program, but there is a grant program, which I think is about $50 million a year. It is a competitive grant program for houses of worship, religious institutions, for their own security.

Mrs. WATSON COLEMAN. Anywhere?

Secretary JOHNSON. Anywhere.

Mrs. WATSON COLEMAN. Thank you. I will have someone to check with your office.

Secretary JOHNSON. My recollection is that it is anywhere, yes.

Mrs. WATSON COLEMAN. Thank you. Thank you.

I am interested in defining this, the individual that is radicalized by home-grown, home-developed, racist-oriented groups and then goes out and commits a crime that results in the loss of life to more than 1 person, more than 4 people. For instance, the Mother Emanuel situation, we understand that this gentleman had been radicalized or had been influenced by some groups—I don't know how you characterize them, I characterize them as racist—and that his intention was to start a race war.

So, Director Comey, I believe that you characterized what happened as a hate crime and this individual as a violator of a hate crime. As you look at it now, is he also a terrorist? Does he legitimately fall into that category?

Mr. COMEY. I want to be very careful what I say about the Charleston killer because he has two death penalty trials coming up.

I said at the time it was for sure a hate crime. As you know, when we investigate, it makes no difference what the label might be on it at the beginning, we investigate it in the same aggressive way. It was for sure a hate crime. What we are trying to untangle was, was there also some domestic terrorism element to that, the definition of domestic terrorism being acts of violence directed at other humans for the intention of coercing a Government or a civilian population.

So we look at both when we investigate a case like that. I don't want to say at this point, given this pending trial, what we concluded there yet.

Mrs. WATSON COLEMAN. One of the concerns that I have is that there are people who are influenced by these groups that hate African Americans or hate Muslims or hate gay community members and have a political agenda to eliminate as many of them as they can.

So to me, it would be very important to have resources in both, Director, in your hands as well as the Secretary's hands, to identify, to categorize, and to respond to and to develop programs that address that kind of terrorism. I am not certain that we do, because we keep talking about ISIL, ISIL this, ISIL that, but we don't necessarily drill down to these areas.

So both you, Mr. Secretary, and you, Director, I would like to hear your thoughts on that.

Mr. COMEY. Well, what I would be happy to arrange for you, Congresswoman, is a briefing on the Domestic Terrorism Section of the FBI's Counterterrorism Division. Our Counterterrorism Division has two parts: International terrorism and domestic terrorism. We have an enormous amount of resources directed to understanding the threat from just those kind of groups, motivated by all kinds of bias and hatred to try and kill people or damage institutions.

So I ought to arrange for you—we have people who wake up every day worrying about those groups and working with the

Southern Poverty Law Center, working with other groups to get information on them so we can disrupt them.

Mrs. WATSON COLEMAN. So will you be sharing that information back and forth with Homeland Security, because they do present a threat to the homeland?

Mr. COMEY. Yes. We work them through our joint terrorism task forces. So it is part of the joint work we do together.

Secretary JOHNSON. Congresswoman, the only thing I will add to that is the manner in which we approach and deal with communities, basically honest, peaceful communities, in which an international terrorist organization is trying to recruit, that is different from trying to approach an organization that by its mission doesn't want to deal with the U.S. Government and may have a violent purpose.

So those require different approaches. One, I think, is more a matter for law enforcement. Another is, I think, more a matter of our community engagement efforts. So they are fundamentally different.

Mrs. WATSON COLEMAN. Just in closing, and there is also that third element that is not just anti-Government, but biased, racist, and what have you, and that represents a threat and a terrorist threat to communities that are nonviolent communities, that are peaceful communities. That is related to a political agenda and it does disrupt and impact individuals as well as government.

Thank you very much. I yield back. Thank you.

Chairman MCCAUL. Thank you.

The gentleman from Texas, Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Chairman.

I appreciate all the witnesses being here today to talk about our National security.

I want to start with you, Director Comey, and ask you about the decision-making process at the Department of Justice and the FBI regarding Secretary Clinton's private email server. You and I had the privilege to serve together at the Department of Justice, an organization whose reputation for integrity is something that I know we both care deeply about.

After Attorney General Lynch and her husband met privately with Bill Clinton on a tarmac in Phoenix, she publicly acknowledged, in her words, that she may have cast a shadow over the integrity of the Department and the investigation into Mrs. Clinton's private email server, but then she didn't recuse herself.

Now, I really can't imagine a situation, either in your prior service as the deputy attorney general of the United States or your current role as the FBI director, where you would find yourself having a private 30-minute conversation with the spouse of a target or subject of a pending Federal investigation a week before you made the decision or recommendation about whether or not to prosecute that person. But if you had been, is there any doubt in your mind about whether or not recusal would have been appropriate or necessary?

Mr. COMEY. That is a question I can't answer. I never discussed with the Attorney General how she thought about that issue. Each recusal situation, as you know, from being a U.S. attorney, is a dif-

ficult and fact-specific one, so hard for me to answer in the abstract.

Mr. RATCLIFFE. Were you surprised at her meeting with the former President?

Mr. COMEY. Well, I think she herself said that it was a mistake and something she wished hadn't happened, and that makes good sense to me.

Mr. RATCLIFFE. So did Attorney General Lynch's failure to recuse herself factor at all into your decision about holding a separate press conference or factor into the timing of the press conference that you held about the FBI's recommendation in the case?

Mr. COMEY. It had no impact on the timing whatsoever. That was driven by the case. It did have an impact and reinforced my sense that it was very important that the American people hear from the FBI on this issue and get as much transparency as possible, because I didn't want to leave a lingering sense that it wasn't doing in a professional, apolitical, honest way.

Mr. RATCLIFFE. You talked a lot about precedents and the lack of a precedent in connection with the decision in this case. Are you aware of any precedent in your time at the Department or at the FBI for an attorney general publicly stating that he or she would accept the recommendation of the FBI and its investigative team without any prior briefings about the evidence or a briefing on their conclusions about the evidence?

Mr. COMEY. I don't know of another circumstance like this that resembles this in any way, and I mean that in a variety of senses.

Mr. RATCLIFFE. Well, here is what I don't get, Director Comey. If Attorney General Lynch was going to accept the recommendation of the FBI, a recommendation that you made on July 5, then why was there a need for a meeting with her on July 6 when she announced her decision?

Mr. COMEY. I think what she said was she would accept the recommendation of the FBI and the career prosecutors. So the meeting, which I attended, was among the FBI team and the career prosecution team to lay out for her what we had found and for them to offer their legal analysis. So I think that was the embodiment of the recommendation that she then accepted.

Mr. RATCLIFFE. Then she would make the decision?

Mr. COMEY. Right. I think that is what she said and what she did.

Mr. RATCLIFFE. How long was that meeting? She said she met with you late in the afternoon.

Mr. COMEY. I think it was at least 90 minutes.

Mr. RATCLIFFE. Ninety minutes.

Mr. COMEY. My meetings all seem to be long these days. It was at least 90 minutes.

Mr. RATCLIFFE. So the person who wouldn't recuse herself so that she could make the final decision about the prosecution a week after she met privately with the spouse of the subject of the investigation took 90 minutes to weigh the evidence collected by more than 100 FBI agents over a year-long investigation involving thousands of man-hours. Is that accurate?

Mr. COMEY. The lawyer in me is objecting to the form of the question, but I will do my best to answer it.

She got a brief, I think a pretty thorough brief on the facts and the law. As I have said to many folks, even though I know folks have strong feelings about this, this was not a cliffhanger from a prosecutive discretion position. My firm belief after doing this for 30 years is that no reasonable prosecutor would bring a case here.

So I think she decided and it looked to me like 90 minutes was adequate to give her the picture she needed.

Mr. RATCLIFFE. In that 90 minutes, did she review the 110 emails that you outlined as being either Top Secret, Secret, or Confidential that were on Mrs. Clinton's—sent or received on her email server?

Mr. COMEY. I don't think it is appropriate for me to talk about the specifics of that meeting.

Mr. RATCLIFFE. I don't want to know about the content. I just want to know whether she reviewed those emails at a minimum.

Mr. COMEY. I think that would be about the content of the meeting, though. Look, I am trying to be maximally transparent, as you can tell, in ways that are unprecedented. I don't think I should get that specific, though.

Mr. RATCLIFFE. Well, I do thank you. I am grateful for your service in the past, present, and in the future to our Nation.

With that, I will yield back.

Chairman MCCAUL. The Chair recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

I think I would like to get a couple of things out of the way before I start. I will say, Benghazi, Benghazi emails, and the tarmac meeting. Now to the serious business.

Mr. Comey, Mr. Johnson, Mr. Rasmussen, let me just say I really want to thank you for your service to this Nation. I think, in the face of the odds that you have been up against, you have done an incredible job in your service to this Nation, and I thank you. I thank all of you.

I have several questions that I would like to ask. You know, today is probably the last day before the House goes out for the summer, and there are just so many things that we have not done for the American people. You know, the Americans are looking to Congress to do something to address the availability of military-style firearms to dangerous people, and that has been our contention all along. I have always worried about what transpired in Dallas happening to our police departments all across the Nation. It was my biggest fear and nightmare. When I talk to the police departments that I have been involved with back in my district, this was always my contention, that these weapons would potentially end up being used against them.

Secretary Johnson, you said that gun control is part and parcel of homeland security. Can you speak to how we can put in place sensible gun legislation in the way that will make this Nation secure?

Secretary JOHNSON. In general, I believe that we should make it more difficult for a terrorist to possess a gun in this country, and I think that there are ways, on a bipartisan basis, we can agree upon legislation to do that. There are presently statutorily-prescribed bases for denying a gun purchase, which the FBI well

knows about. What we lack right now is the discretion to deny a gun to somebody who meets certain specific criteria that matches one of our different lists. Legislation to do that coupled with a prescribed adjudication process—so that if the purchaser takes issue with the denial, they have the ability to challenge that—I think is, in general, a good idea. There is legislation pending in this Congress now to try to accomplish those things, and I hope that Congress continues to work at that.

What I meant when I said—what I meant was that we have to face the fact that sensible gun control consistent with the Second Amendment is not just a matter of public safety; it is a matter of homeland security too when you look at San Bernardino and when you look at Orlando and the weapons that were used in those attacks.

Mr. PAYNE. Right. Thank you.

Director Comey, by law, the NCTC serves as the primary organization in the U.S. Government for integrating and analyzing all intelligence pertaining to counterterrorism, except for the information pertaining exclusively to domestic terrorism. Because of its lead status for counterterrorism investigations in the homeland, the FBI arguably serves the parallel role for the domestic terrorist threat. The development of any interagency regime for collection and analysis of domestic terrorism information might start with the Bureau's capacity in this regard. What resources have the FBI allocated and expended in the collection and analysis of domestic terrorism-related intelligence as well as for safeguarding civil rights as well?

Mr. COMEY. Well, as I said earlier, Congressman, it is a huge feature of the work of our counterterrorism division. We have hundreds of people who work on what we call the DT side, that is, at headquarters agents and analysis, and then, in every field office, there are agents and analysts who focus just on that domestic terrorism mission. So we have extensive resources devoted to it all over the country.

Mr. PAYNE. Thank you.

You know, Secretary Johnson, everybody is saying this is potentially the last time you will be before us. Are we safer now than we were when you started?

Secretary JOHNSON. Good question. I think that the environment has changed fundamentally from where it was 3, 4 years ago. My first 4 years in this administration in the Department of Defense, I was giving the legal signoff on a lot of targeted lethal force at terrorist organizations overseas to prevent them from exporting terrorism to our homeland, and I think we did a pretty good job of degrading a lot of the threats that we saw at the time. We continue to do that in places like Iraq and Syria.

Now we have got to deal with terrorist-inspired attacks, terrorist-enabled attacks, people who live here, who were born here who are recruited, inspired by terrorist organizations through social media, and that is a challenging environment, and that can happen with little or no notice to our intelligence community, to our law enforcement community, which requires, in my judgment, a very different kind of approach, not just militarily, not just through law enforcement, but through our CVE efforts, through public awareness, pub-

lic vigilance. I said in my opening remarks that the prospect of another attack by a self-radicalized actor, someone inspired by a terrorist organization is the thing that most keeps me up at night. So, in that respect, that is a new threat that we weren't dealing with on a regular basis as recently as 4, 5, 7 years ago, and it is something that I hope that, in the Executive branch and in Congress, we will continue to dedicate ourselves to combating.

Mr. PAYNE. Well, thank you very much. You will be missed. Thank you.

Chairman MCCAUL. The Chair recognizes the gentleman from New York, Mr. Donovan.

Mr. DONOVAN. Thank you, Mr. Chairman.

Let me add my congratulations, gratitude for your commitment and dedication, the three of you, to the safety of our Nation. Because you come before us so many times, we have become very familiar with you. Jeh and Jim have been friends from back in New York for a very long time. One of you will appear before this committee again; one of you this may be your last appearance. Since I am up for reelection, I hope it is not one of my last appearances before this committee.

The Chairman is very proud when he tells our Nation so many times that this committee has passed more legislation in this Congress than any other committee in Congress outside of Energy and Commerce. All of that legislation, most of that legislation, maybe all of that legislation, results from testimony before us from witnesses like yourself, your expertise, sharing with us your concerns.

I have read all of your written testimony. Believe it or not, we actually do read that. Particularly, in Director Comey's testimony, he stresses that, in combating terrorism through social media, we are doing everything we can within the laws and in respecting people's privacies.

Is there something that you see as a tool that would be helpful to each of you that either your legal teams are looking at that we can help you? What other tool can we give you that will make your job more effective as you respect the laws of our Nation, as you respect the Supreme Court's decisions, interpretations of our laws? What can we get out of this hearing today that, if we are able to pass legislation, will allow you to do your job more efficiently? I ask that for the three of you. I know the votes are in 15 minutes, so I want to get my colleagues to ask their questions as well.

Secretary JOHNSON. Congressman, two things to come to mind immediately, one of which has already been passed out of this committee, specifically, authorizing joint task forces within my Department for border security. That is something that I know this committee supports and has been passed by the full House. I am hoping through one vehicle or another, it passes the full Senate as well. Joint task forces for border security help combat illegal immigration as well as narcotics, and there are certain legal limitations I am finding to fully implementing the joint task force concept for my Department.

The second thing, which I have spoken to several of you about, is specific Congressional authorization to reorganize our National Protection and Programs Directorate into a cyber and infrastructure protection agency. We need an agency for our cybersecurity

mission more closely aligned with the protection of our critical infrastructure, and that is something that I think will go a long way to streamlining our cybersecurity and critical infrastructure protection mission. So those are two things that come to mind immediately.

I want to agree with what you said at the outset about how impressed I am with the productivity of this committee. Just in the time I have been Secretary, this committee has pushed out legislation on cybersecurity, aviation security that I think really has helped to strengthen the homeland. So thank you.

Mr. DONOVAN. We want to continue to do so.

Yes, Director.

Mr. COMEY. I will give you two quick ones. One is an enormous issue that this committee is thinking about, I think, in a good way. We have to deal with the challenge of encryption and its impact on our criminal justice work and our National security work. The needles we are looking for are becoming invisible to us in case after case after case, and that is a big problem.

Second is a—seems like a small thing, but we have made it, I believe, accidentally harder in our National security investigations for our agents to use the process we use to get telephone information, to get similar information on the internet. The Senate is focused on this. I don't believe that it was intended by the legislation to make it that hard for us or is it justified by any reasonable concern about privacy. That is called the ECTR fix. We have got to fix that.

Mr. DONOVAN. Thank you very much.

Director.

Mr. RASMUSSEN. I would just associate myself with Director Comey's remarks about encryption. As you noticed, I highlighted that in my opening testimony as well.

Beyond the productivity of the committee that Secretary Johnson referred to with your legislation, I would also like to say that we in the Executive branch also take note of some of the staff-driven reports that have been produced on key substantive issues as well, like foreign fighter flows and whatnot, and I know we work closely with the committee staff to support that work, and it actually does assist us as well.

Mr. DONOVAN. I thank you all.

Mr. Chairman, I yield the remainder of my time.

Chairman MCCAUL. I appreciate it. If I could just quickly comment, it is very important, these three major items: The commission to deal with encryption, we are hopeful the Senate will take that up and mark that bill up. That is critically important.

Director Comey, you and I understand the gravity of this issue.

NPPD, as the Secretary has requested, is being held up by 4 other committees in Congress. That is a problem with the jurisdiction that I think needs to be fixed. Then, finally, on the border joint task force, it is my sincere hope we can add that into the NDAA bill, as I will be on the conference committee for that.

So, with that, let me recognize Mr. Perry from Pennsylvania.

Mr. PERRY. Thank you, Mr. Chairman.

Gentlemen, thank you for your service to the country. We are all counting on you. I am thinking, with the Ranking Member's re-

marks about hearings in the late—well, early and late 1950's regarding the infiltration of communism into our Government, and I just want to reflect on that a little bit. Although the methods by most Americans were objectionable, in retrospect, the information was almost all completely accurate even though the individual, Senator McCarthy's, reputation was destroyed. We lost sight of what he was really talking about for the methodology, and we are just—I just want to beseech you that we are counting on your integrity and your diligence in keeping our country safe.

With that, Director Comey, I don't know exactly how you characterized it, but you said recently that the FBI is ineligible for contact with CAIR? Maybe it is not ineligible. What is the terminology? You don't have contact with CAIR based on the Holy Land Foundation investigation and their ties to terrorist extremist organizations, mosques, et cetera?

Mr. COMEY. Yes. Our policy is that we will not do work with CAIR; that is, sponsor events, do joint events. If a CAIR representative happens to come to some other event that is being sponsored some other way, we don't kick them out, but we don't work, as we do with so many other groups, nonprofit groups, to sponsor activities with that group.

Mr. PERRY. So there are reports or conjecture at least that there was some involvement with the Bureau in the selection—and CAIR in the selection of FBI witnesses to interview at the Fort Pierce mosque regarding the Orlando massacre. Is there any truth to that?

Mr. COMEY. I have never heard that.

Mr. PERRY. OK. So, at this point, you don't know anything? You have never heard that. You know anything about that. I think you would refute that, generally speaking——

Mr. COMEY. Yes.

Mr. PERRY [continuing]. Otherwise——

Mr. COMEY. I mean, I am sitting here, I guess anything is possible, but——

Mr. PERRY. Right.

Mr. COMEY [continuing]. I have not heard that, I have no reason to believe that that is true.

Mr. PERRY. OK. And——

Mr. COMEY. I would think that I would have heard that.

Mr. PERRY. All right. Thank you. If I can find a source for that, I will write you and ask for that particularly so we can get to the bottom of that.

Mr. Johnson, in a recent Senate hearing, there was a CBP Officer that made a claim regarding the Department's ending or stopping the collection of data and the destruction of databases regarding Islamist supremacists that he believed might have been able to prevent the San Bernardino attack, and you said at the time, if I recall, that you hadn't looked into those charges. I am just wondering, in the intervening time period, have you looked into them, and do you plan to?

Secretary JOHNSON. Well, the questioning 2 weeks ago from Senator Cruz was regarding the testimony of Mr. Haney that, across the Executive branch, we had somehow purged certain words in our dialog. That is what Senator Cruz asked me about. I had not

heard about that before, and, frankly, given everything that is happening with Dallas——

Mr. PERRY. Sure.

Secretary JOHNSON [continuing]. Orlando, Ataturk Airport, I have not had the opportunity to personally sit down and look into Mr. Haney's allegations, and I hope you can understand why.

Mr. PERRY. I do understand. I think it was regarding databases and connecting the dots, which would lead to another question. So it is not just about terminology. If you could, please, sir, take a look into that. I know you have got, at least by your clock, a limited amount of time left, and——

Secretary JOHNSON. One hundred ninety days.

Mr. PERRY. But who is counting, right? I know you have got some significant issues right in front of you, but we would like to know the outcome of that questioning regarding the purging of those databases and the connecting of the dots, if you could, sir.

Also, I think at the time, you said that you thought your personnel were smart enough to connect the dots between terrorism and things like Sharia adherence, jihad, and Islamic supremacism more generally, and I would agree with you. It is not a question of if they are smart enough. The question is whether it is a career-ending offense, as Mr. Haney might assert that it has been, and if there are constraints in those connections of the dots at your organization, if there is a policy of constraint.

Secretary JOHNSON. What I was referring to 2 weeks ago was the work actually of those who work for the people at the table here with me. In my observation, NCTC, the intelligence community, my people, the FBI do an excellent job of working together to track terrorist threats, plotting against the homeland, whatever it is labeled. So what I said then, which I will repeat, is I don't think that our personnel become too bogged down in the particular label we choose to put on a terrorist actor. They are more interested in the substance of what that person is doing.

Mr. PERRY. I am not here to discuss the labeling. You and I have had that discussion before, probably have a bit of a disagreement, I accept that at this point, but what I am discussing and what I want to ask you directly, is there a prohibition, is there any policy toward the work that Mr. Haney was doing such that current individuals in your Department in particular would see that as somehow bad for their career, or they are dissuaded from doing, or they are prohibited from doing that?

Secretary JOHNSON. My honest answer is I have not had an opportunity to look into exactly what Mr. Haney——

Mr. PERRY. OK.

Secretary JOHNSON [continuing]. Alleges, though I gather he has written a book and he has been on TV.

Mr. PERRY. I haven't read the book, but——

Secretary JOHNSON. It is something that I—it is something that I am interested in learning more about.

Mr. PERRY. So, regarding the database and regarding the previous question about the policy, could you give us a written response to that when you have time, assuming you have time——

Secretary JOHNSON. Yes.

Mr. PERRY [continuing]. Before you leave?

Secretary JOHNSON. Yes.

Mr. PERRY. Thank you, sir. I appreciate it.

I yield back.

Chairman MCCAUL. Mr. Katko from New York is recognized.

Mr. KATKO. Thank you, Mr. Chairman.

I echo the sentiments of many of my colleagues on the panel here in thanking all of you for your fine service to this great country. Mr. Comey, I wasn't the hotshot you were at the time at the Department of Justice, but I served with you for many years as a Federal organized crime prosecutor, 20, as a matter of fact, and I have always admired your skill and grace. While I don't always agree with you on things, I do admire your service to our country, so I thank you.

Now, Secretary Johnson, I want to—as my Subcommittee on Transportation Security, we have direct oversight over our airports both Nationally and internationally, and including last-point-of-departure airports, and as you know, one of the last-point-of-departure airports that is looking to be opened is in Cuba, and there are 10 of them, which is an extraordinarily large amount of last-point-of-departure airports. During our investigation in looking into this matter in our oversight capacity, many concerns have developed. No. 1, do the airports have the capacity to handle the 110 flights a day that are being contemplated to and from the United States; concerns about the equipment, you know, whether they even have body scanners or whether they are going to have body scanners, whether they are going to have document verification machines, whether they are going to have all the tools of the trade that we have here, explosive trace detection equipment and what have you? Those are all concerns we have.

The training and vetting of employees is another area of concern, and a huge concern for us, especially with the insider threat, as evidenced in Sharm El Sheikh and Mogadishu with the downing of the airplanes.

Canines is another area of concern.

Another area of concern is whether the TSA is going to have access to these airports, given the embargo against Cuba and given the current state of the diplomatic relations.

Overlaid with all that, Mr. Secretary, last year, Cuba was taken off the list of terrorist countries. One of their best buddies is still North Korea.

Another thing that is a major concern to me is that Cuban visas are showing up in the Middle East. A *Washington Post* article from April 17 of this year, which I ask to be incorporated into the record, evidences that these visas are suspected to being produced in Iran and other countries.

[The information referred to follows:]

ARTICLE SUBMITTED FOR THE RECORD BY HON. JOHN KATKO

KABUL LIBRE! ONE NEW AFGHAN TRAIL TO THE WEST GOES THROUGH CUBA

By Tim Craig, April 17, 2016.

KABUL.—With roads to Europe increasingly blocked by strict border controls, Afghans hoping to flee war and economic peril are desperately searching for new escape routes by way of refugee camps in India, airports in Russia and even the beaches of Cuba.

The shifting travel plans—which are also seeing Afghans attempting to buy their way into Europe before leaving Kabul, through the purchase of visas—may signal the next phase in a migration crisis that is rattling world leaders and draining Afghanistan of its workforce.

After a year in which hundreds of thousands of Afghans poured into Europe by land, more migrants are now trying to skirt hostile border agents and dangerous boat trips by flying to their destinations. As a result, although human smuggling was a booming industry in Afghanistan last year, criminal rackets that trade in visas may be reaping a windfall this year.

"People now are not willing to take great risks," said Tamin Omarzi, who works as a travel agent in Kabul's largest mall. "They want to just travel with a passport, and don't come back."

Last year, along with more than 1 million refugees from Syria and Iraq, about 250,000 Afghans journeyed to Europe in hopes of securing asylum there. Many traveled through Iran and Turkey before crossing the Aegean Sea to Greece.

Overwhelmed by the influx, European leaders have shown less sympathy for Afghans than for refugees from Syria and Iraq. Much of Afghanistan, they note, remains under the control of a Western-backed government.

Last month, the European Union reached a deal with Turkey to send migrants back to refugee camps there, effectively severing the land route to Europe.

Since then, travel agents in Kabul report that requests for visas to Iran and Turkey are down by as much as 80 percent compared with last year at this time. A United Nations report released Thursday also concluded that the flow of migrants from Afghanistan has slowed while "people reconsider destinations and subsequent optimal routes."

"There is currently lower movement but no dropoff in the people wanting to go," said Alexander Mundt, assistant representative for protection at the U.N. refugee agency. "They are just exploring their options, their means and the right moment to go."

Plenty of Afghans are still on the move, however, in a mass migration that is raising new challenges for immigration agencies across the world.

Sulaiman Sayeedi, a travel agent in Kabul's middle-class Wazir Akbar Khan neighborhood, said there has been a surge in demand for flights to India, Indonesia, and Central Asian countries such as Tajikistan and Uzbekistan.

Once they arrive, Afghan travelers often claim refugee status with the United Nations in hopes of being resettled. In India, for example, Afghan asylum applications have doubled in recent months, according to Mundt.

Other Afghans are flying to Moscow, believing that from there they can cross into Ukraine or even Belarus and then move onward to E.U. countries.

"Some people are coming in and just asking for tickets to anywhere they can get to," Sayeedi said. "They just want a better life, a more civilized, modern life."

To achieve that in the United States or Canada, Afghans may make Cuba their gateway to the Western Hemisphere.

Over the past 2 months, travel agents in Kabul have been surprised by Afghans showing up at their offices with Cuban visas, which are suspected of having been issued in Iran or acquired on the black market.

"Ten or 15 people have come just since January asking for tickets for Cuba," Sayeedi said. "And they are not staying there. The only option is to move forward, probably on to Mexico and then America or Canada."

Other agents in Kabul also report a spike in interest in Cuba, and U.N. officials in the northern Afghan city of Kunduz say they recently encountered a family with Cuban visas. Havana has been a way station in the past for South Asians hoping to transit to Central America and from there to the United States.

Besides Cuba, some Afghans are attempting to land in South America, either to seek residency there or make the trip north toward the U.S.-Mexico border.

Rahimihi, a travel agent in Kabul's central Shar-e Naw district, recently booked flights for relatives who had obtained visas for Ecuador, as well as transit visas through Brazil.

"They first had to go to Pakistan to get the transit visa [from the Brazilian Embassy], and then left 2 weeks ago," said Rahimihi, who, like many Afghans, uses only one name. "They want to go to Canada."

But central and northern European countries remain Afghans' preferred destinations, reflecting the widely held belief here that Germany, Norway, and Sweden are the most welcoming toward refugees.

Mohammad Unus has been deported from both Italy and Turkey over the past 2 years while attempting to reach Germany. Now, for his third attempt, he's working with a local travel agent.

"Since Ashraf Ghani became president, all the people want to escape from Afghanistan," Unus said, reflecting widespread concern here that Ghani's promised economic reforms haven't materialized. "I've already spent $40,000 trying to get to Europe, and now I plan to sell my house to get there if I have to this time."

Such desperation is fueling the shady enterprise of visa dealing on the streets of Kabul.

According to travel agents, Afghans are now paying dealers $15,000 to $25,000 to obtain a "Schengen visa"—a reference to countries that are part of the Schengen Agreement, which was drawn up to allow unrestricted movement among 26 European nations. The business continues even though seven of those nations, including Germany and Sweden, have re-imposed temporary border controls.

The visa dealers work directly with rogue staffers at European embassies who issue the visas for a kickback, the agents claim.

"You never know who is doing it on the inside, but it's someone with a soft heart who is approving these documents," said Peer Muhammad Roheen, managing director of Air Gateway Travel and Tours in Kabul.

One travel broker, who spoke on the condition of anonymity to discuss his sensitive business, said Afghans even with modest means are now turning to visa dealers because "people now prefer to go by air to Europe directly."

"If you got good contacts inside the embassy, you can get it done in 1 week," the broker said.

When visa dealers fail to obtain valid visas, they sometimes turn to even more elaborate schemes, according to travel agents.

Legal residents of Europe, for example, are being paid to travel to Afghanistan or Pakistan and then give their passports to Afghans with similar physical characteristics, said Mustafa, a travel agent in southwest Kabul who also uses only one name. The person who gives up the passport then claims it was lost or stolen.

"People will pay, and those short on cash will sell anything they have," Mustafa said.

But U.N. officials question how many Afghans will be able to afford expensive options for fleeing.

"The people with that kind of money to spend are already gone," Mundt said, adding that many of those now trying to flee are poor and middle-class families. "They may still have some means, but maybe $6,000 to invest and not $20,000."

The recent outflow of wealth and talent from Afghanistan has alarmed Ghani, who has been urging Afghans to stay home.

But until stability returns, travel agents expect to stay busy planning one-way trips.

"For survival, people will do anything," said Roheen, who estimates that 30 percent of urban Afghan youths hope to leave the country. "If they encounter a problem, then they will just try another option."

Mr. KATKO. So we have that.

Then you have the fact that airlines, like I mentioned, are being targeted by ISIS and that Cuba remains friends with North Korea, like I said, and many other concerns.

We are doing the oversight. We wanted to go to Cuba. And as you well know, the Cuban Government, instead of opening their arms and having us come and look at the airports, denied Mr. McCaul's access to Cuba as well as mine and the Congressional delegation. Does that give you any concern?

Secretary JOHNSON. Yes. I was disappointed that the Congressional delegation was not issued visas. The Chairman asked me if I could assist in that matter, and we tried, and we were unable to make that happen. So I am disappointed that the Cuban government did not——

Mr. KATKO. I thought you were all-mighty and all-powerful?

Secretary JOHNSON. I am sorry?

Well, but let me comment more generally, sir, on this last issue of point of departure from Cuba. What I have told our people in TSA is I want an assurance that any last-point-of-departure airport from Cuba satisfies our U.S. screening standards, not just international screening standards. I have also told TSA that I want

them to get with the Cuban Government and put in place agreements, MOUs, for Federal air marshals and hopefully make that happen before we start commercial flights, and I want to see a senior-level official from TSA headquarters personally go down to Cuba to take a look at the security at last-point-of-departure airports.

We are very focused on last-point-of-departure airports, as I am sure you know, particularly in the Middle East region right now. I think we have some challenges there. Since the crash last year in the fall, I have asked our people to focus on airports in that region. We are not going to take our eye off the rest of the world, however. So, Congressman, this is something that I am personally focused on.

Mr. KATKO. I appreciate that. Now, let me ask just a follow-up on one of those questions. If the Cuban Government would disallow Federal air marshals on their flights to and from the United States to Cuba, would that be a deal-killer for Homeland Security?

Secretary JOHNSON. I would have to assess it at the time. We don't have MOUs with every single last-point-of-departure country. We have a number of them now, and we are expanding on that list. I would have to assess it at the time.

Mr. KATKO. OK. One last thing, Mr. Chairman, one quick question. I have a bill that I submitted to Congress yesterday, the last—earlier this week about oversight with the Cuban airports, and it articulates all the concerns and the goals you have. The only other thing it has would be that GAO would do a follow-up review of the analysis to ensure it is accurate before the flights begin. Would you agree with that?

Secretary JOHNSON. Yes.

Mr. KATKO. All right. Thank you.

Chairman MCCAUL. The gentleman, Mr. Hurd, from Texas.

Mr. HURD. Thank you, Mr. Chairman.

Before I begin my questions—and I am going to start with you, Mr. Rasmussen—I would like to make an FYI to the Secretary and the director. You probably already know, there has been a task force that has been created, being chaired by the Chairman of Judiciary and the Ranking Member, on looking at police accountability and aggression toward law enforcement, 6 Republicans, 6 Democrats. We are going to try to do this in a bipartisan way. We are going to try not to retreat to the same tired corners and talking points on this issue, because the reality is, is whether the color of your skin is black or brown or your uniform is blue, you shouldn't be afraid of being targeted when you walk the streets in the United States.

My good friend and fellow Texan Sheila Jackson Lee is on the committee as well as well as my friend Cedric Richmond from Louisiana, and we would welcome you all's perspective and number of years experience in your service to the Federal Government as we pursue this endeavor. It is hard to have a bunch of people together, you know, being in a bipartisan manner, but I think we can do it, because, guess what? Those folks that are trying to sow terror and fear in our hearts, they will not win, and they will not win, because this body is committed to doing this and we have folks like you all on the front line.

Mr. Rasmussen, when I was chasing al-Qaeda when I was in the CIA, I would have loved for al-Qaeda to be using social media the way that ISIS is. It increases the surface area of attack where we can ultimately penetrate and understand the plans and intentions of groups like this. If you were an American walking around in the federally-administered tribal areas of Pakistan and said, "I want to join al-Qaeda," you would likely get your head cut off, but now we are able to target people from the comfort of our homes.

I am not asking to get into Classified information, but has our intelligence on the plans and intentions of groups like ISIS increased due to their use of social media?

Mr. RASMUSSEN. There is no—I like your term the greater surface area that the group occupies because of its presence in all these ways. That certainly provides opportunity, opportunity in all kinds—measured in all kinds of ways for analysis, for operational work. That isn't my responsibility but belongs in the hands of other intelligence community partners. On net, though, I would describe our effort to gain an understanding of ISIL intentions and strategy and direction as being a harder target right now than what we faced with al-Qaeda, and it attaches to a number of issues, the encryption issue that Director Comey has spoken so eloquently on, but also just the fact that ISIL is a savvy——

Mr. HURD. Right.

Mr. RASMUSSEN [continuing]. Experienced adversary that knows who we——

Mr. HURD. So you bring up encryption. I guess this question is to Secretary Johnson. I am with you. I am glad you were able to mention the cyber and infrastructure protection agency. I think it is a critical tool. I agree with the Chairman and support this. We have to get it done now, because if we don't do it now, it is going to be years from now.

I would like to add that the efforts that the Department of Homeland Security NPPD has done across the Federal Government in helping protect the digital infrastructure of our fellow agencies has been impressive.

How important is the use of encryption to make sure that these other agencies are protecting the information that they do have on American people?

Secretary JOHNSON. We are, through binding operational directives, which is an authority that was given to me by Congress, and other things, working with other Federal agencies to secure their own systems. This is a work in progress. I want to see not just the CIOs of each agency but the Cabinet heads, the agency heads——

Mr. HURD. Should they be using stronger encryption to protect digital information or weaker encryption?

Secretary JOHNSON. It is hard to answer in general. I think we need to improve the security of our systems. I think that is the way I would answer it.

Mr. HURD. Director Comey, first off, your level of transparency on what the FBI knew or didn't know around the Orlando killer, I think, was impressive and was important for the American people to know and understand, and I commend you for that.

One of the issues—and I recognize that the Orlando killer cased a number of locations, and it appears that, at many of those loca-

tions, there were private security. Is there a vehicle by which private security is able to—you know, if they see a suspicious activity report, does that go somewhere? Do these private security have training? Is there a way to integrate that kind of information into the JTTF structure, into local police? Your thoughts on that.

Mr. COMEY. Yes. I think it is—they are integrated. There are probably ways to improve it in both directions through their relationship with the local uniformed police. If they see something suspicious, either if they—even if they pass it informally, it is going to get to the JTTF right away. So my sense is it is pretty good through the local police.

Mr. HURD. Mr. Chairman, I would be remiss to not mention and have a comment on encryption. You know, I think it was one of your own employees, Director Comey, who mentioned that our civil liberties are the things that make our country great; they are not our burdens. I agree wholeheartedly with that, and I think that we should be focusing on how we strengthen encryption and not weaken it, and make sure that law enforcement and the private sector are not talking past one another but are actually working together. We also have to ensure that we continue to create a culture within the Federal Government that protects information and protects those secrets that so many people have worked hard to collect.

Mr. Chairman, I yield back the time I do not have.

Chairman MCCAUL. I thank the gentleman.

The Chairman recognizes the Ranking Member for purposes of a closing statement.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

I yield to the gentlelady from Texas.

Ms. JACKSON LEE. I thank the Ranking Member, and I thank her for her leadership, and the Chairman.

Let me quickly—I think my questions may warrant a one-letter—one-word answer. In light of—and, again, Mr. Comey, thank you for your presence at the Dallas memorial. But in light of the existence of weapons of war on the streets, would you and your agents surmise and believe that law enforcement are less safe because AR–15s and others are still about in this Nation in civilian hands who may be doing wrong things, less safe?

Mr. COMEY. The more weapons in the hands of bad people, the less safe our people are.

Ms. JACKSON LEE. Second question is, with the career investigators and prosecutors who investigated former Secretary Clinton on the matters dealing with emails, is it my understanding and your understanding and confidence that you have completed the investigation as well as the Department of Justice?

Mr. COMEY. Yes.

Ms. JACKSON LEE. To your satisfaction?

Mr. COMEY. Yes. It was done in an apolitical, professional way. I am very proud of my folks.

Ms. JACKSON LEE. My last point is—I made a point about swatting. I would appreciate if you could refer me to one of your individuals at headquarters to be able to have that matter addressed as quickly as possible.

I thank you so much very for your service. I know that America is going to be a better Nation because we are all working together in a unified manner.

I yield back.

Chairman MCCAUL. Let me just thank all three of you for your expertise. It has been very instructive to this committee. I want to thank you for your service on all three levels.

FBI, the amount of terrorism you have stopped in this country astounds me, the job your agents do in arresting over 80 ISIS followers since the beginning of the caliphate.

To NCTC, for doing the intelligence fusion, which serves this Congress, I think, and the Executive branch so well.

Finally, to Secretary Johnson, I think this will be your last testimony before this Congress. I think you think that that is for certain, but on a personal level, I have enjoyed working with you. I want to thank you for your service both to the Department of Defense, doing very important work targeting the threat where it exists, but also as Secretary of Homeland Security, you have truly served with honor and distinction, and we thank you for that.

With that, this hearing stands adjourned.

[Whereupon, at 12:39 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM RANKING MEMBER BENNIE G. THOMPSON FOR HON. JEH C. JOHNSON

COUNTERING VIOLENT EXTREMISM

Question 1a. Federal efforts directed at Countering Violent Extremism (CVE) often depend on Government agencies cooperating with local groups. The administration highlights a "community-based approach" for the Federal Government. According to the administration, the Federal Government most effectively acts as a "facilitator, convener, and source of information." As such, to date the bulk of Federal-level CVE work has revolved around community engagement. The Department of Homeland Security has yet to release a CVE strategy; however, it has stood up an Office of Community Partnerships.

Please detail some of the programs that this office will implement.

Answer. The Office of Community Partnerships (OCP) is focused on partnering with and empowering communities by providing a wide range of resources to use in countering violent extremism. OCP does this by equipping State, local, Tribal, and territorial governments, community organizations and other partners with necessary information, grants, tools, and training to help them identify and counter radicalization to violence.

OCP's major objectives include: Increasing access to grants for CVE initiatives, community engagement, tech-sector engagement to empower credible voices in communities vulnerable to violent extremism, field support training to better support local communities and law enforcement engaged in CVE efforts, and philanthropic engagement to facilitate long-term partnerships with communities.

DHS released a comprehensive CVE strategy on October 28, 2016 which will also be provided to you.

Question 1b. Will these programs extend beyond the current focus on Muslim communities?

Answer. Violent extremism in all its forms poses a persistent and unpredictable threat to the homeland and may come from a range of groups and individuals, including domestic terrorists and home-grown violent extremists. As such, DHS has designed a countering violent extremism approach that addresses all forms of violent extremism, regardless of ideology, focusing not on political, cultural, or religious views, but on preventing violence.

Question 1c. What resources will this office receive in terms of staffing and operating budget and will those resources be diverted from other programs and offices?

Answer. For fiscal year 2016, the Office of Community Partnership (OCP) received $11.3 million and 12.5 full-time equivalent. This amount represents $3.1 million originally enacted and $8.2 million in transferred funds to OCP for Countering Violent Extremism activities. The fiscal year 2017 President's budget requests $3.5 million and 16 full-time employees for OCP. All resources and personnel initially associated with the foundation of OCP are fully supported by the OCP budget. Due to the expertise they bring, OCP continues to utilize approximately 6 detailees (1 OPE, 1 I&A, 1 USCIS, 1 TSA, and 2 CRCL) from within the Department.

Question 1d. Which domestic terrorist ideologies does the DHS Office of Community Partnerships focus upon?

Question 1e. Which communities do you intend to engage regarding issues surrounding non-jihadist terrorism?

Answer. *OCP and DHS Headquarters Efforts.*—DHS I&A has a team of analysts whose sole focus is domestic terrorism analysis. These analysts are experts in all the disparate categories of domestic terrorism—such as violent white supremacist extremists, violent sovereign citizen extremists, violent anarchist extremists, and violent environmental/animal rights extremists.

The Department provides training for law enforcement; delivers briefings to fusion centers, law enforcement, and communities; develops research on preventing and further understanding the phenomenon of radicalization to violence; and develops analysis on the spectrum of domestic-based threats.

OCP Field Efforts.—DHS OCP provides direct support via field staff in a couple of regions. For example, in Colorado, DHS OCP and the U.S. Attorney's Office (USAO) have partnered to counter all forms of violent extremism. Colorado has experienced both international violent extremist incidents, with 3 teenage girls attempting to join ISIL in October 2014 and another young woman attempting to join in April 2014, as well as incidents of domestic violent extremism, like the Planned Parenthood shooting in November 2015, and several incidents of sovereign citizen extremist violence. DHS OCP and USAO have focused on prevention (through awareness-building and counter-narratives) and intervention. Together they are developing a community awareness briefing (CAB) that builds comprehensive awareness of all forms of violent extremist activity that has occurred in Colorado, both domestic and internationally inspired.

DHS OCP and USAO have presented multiple CABs to Muslim American leaders and parents to build awareness of ISIL and related groups. After expanding the CAB to include information on domestic violent extremism, they have delivered this new presentation in Colorado Springs to Christian communities on June 4 (who expressed interest after the Planned Parenthood shooting), and to gang prevention and intervention partners in the Gang Reduction Initiative of Denver (GRID) program on June 21.

DHS OCP and USAO have put on multiple Protecting Houses of Worship events throughout the State to multiple faith communities on how to respond to threats to their centers. USAO started these after the Charleston AME Church shooting, which involved persons believed to be motivated by a white supremacist extremist ideology. These briefings include information on all types of violent extremists that have committed acts of violence.

DHS OCP and USAO are working with local partners to institute an intervention model in Colorado to address all forms of violent extremism. This is still in the beginning stages, but the model will be set up to address all forms of violent extremism, and will complement existing models to prevent gang activity and school violence.

Question 2a. The CVE community has struggled with measuring the effectiveness of its efforts.

How can the CVE community develop useful metrics?

Question 2b. What metrics are most useful to you in determining whether the Department's CVE actions are having the desired impact on the adversary and on our security more broadly?

Answer. Developing measures of performance, effectiveness, and benchmarks for CVE programs and initiatives remains a top priority for the Office for Community Partnerships and the CVE Task Force. Academic partners, such as the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START), have published comprehensive reviews of program evaluation across a range of CVE initiatives. The National Institute of Justice is another Federal partner which has spearheaded efforts to fund evaluations of CVE programs, and they have just released a new assessment of a U.S.-based CVE program in Montgomery County, Maryland. In addition, DHS's Directorate of Science and Technology is completing CVE program evaluations of CVE efforts in Los Angeles and Boston; final reports for this project are will be finalized and published in early 2017.

Federal departments, agencies, and non-governmental experts involved in CVE programming are currently involved in a robust conversation and information exchange on these issues. For example, the State Department has developed a useful guide for practitioners as they develop measures to assess CVE programs, which has been shared across the interagency and with CVE practitioners.

With regard to the assessment of individual CVE programs, program metrics will be required for all Federally-funded CVE programs and will be tailored to each specific initiative before programs are launched. The CVE Task Force will work to coordinate these efforts. Examples of program metrics include developing a logic model as well as providing both output measures (e.g., numbers of individuals who have participated or number of products developed) as well as impact metrics (e.g., percent increase in knowledge, percent increase in awareness or percent increase in trust developed between communities and law enforcement). These program evaluations in diverse fields of practice like community policing, gang interventions, and public health initiatives provides strong evidence-based assurance that our Federal investment is being directed in the most effective ways.

Question 3. Please provide us with a time line for when CVE grants will be awarded. What types of activities to you anticipate the grant funding will support and how did the Department go about identifying the activities that would most effectively counter violent extremism?

Answer. DHS anticipates that funding selection will occur in January 2017. The grant funding will support activities in 5 focus areas: Developing resilience; training and engaging with community members; managing intervention activities; challenging the narrative; and building capacity of community-level non-profit organizations active in CVE. These focus areas are based on research, analysis of the current gaps, and which CVE activities needs grant funding versus some other type of support. Additionally, through the competitive application process, the program encourages innovation and whole-of-society partnerships. As noted in the Notice of Funding Opportunity, senior leadership from the DHS Office for Community Partnerships, FEMA, the DHS Office for Civil Rights and Civil Liberties, and the CVE Task Force (which includes NCTC, DOJ, and FBI) will review all scoring results and will make recommendations on which projects, or portions of projects to fund in order to maximize the total impact of the available funding including removing from consideration applications that do not propose as large an impact relative to their costs in comparison to other applications or are duplicative of higher-scored applications. The results of the senior leadership review will be presented to the Director, Office for Community Partnerships and the assistant administrator, FEMA GPD, who will recommend the selection of recipients for this program to the Secretary of Homeland Security. Final funding determinations will be made by the Secretary of Homeland Security, through the FEMA administrator. The Secretary retains the discretion to consider other factors and information in addition to those included in the recommendations.

CYBERSECURITY

Question 4a. The rising number of connected devices means a potential wider attack surface, and there has been some speculation that the Internet of Things is the new frontier of ransomware attacks.

How credible are these concerns, and how does the Department plan to assist small business, in particular, Main Street businesses, in dealing with this new threat?

Question 4b. What role should the Government play in the securing the Internet of Things?

Answer. The Internet of Things (IoT) is a broad term to describe the proliferation of categories of devices that are connected to the internet, to include, for example, self-driving cars, "wearables" that track heart rates and calories burned, and medical devices that transmit health information in real time. Growth of the IoT presents extraordinary opportunity for consumers and businesses, but that opportunity is accompanied by the cybersecurity risk with any connected network or device. A 2014 study by the President's National Security Telecommunications Advisory Committee (NSTAC) highlights the growing security threats that government and industry must consider with the IoT: "an exponential expansion in attack surfaces, a changing threat landscape, privacy concerns, an increased potential for kinetic-focused cyber attacks, and changes to the hardware life cycle." DHS agrees with the finding in the NSTAC report.

When considering smaller cities, municipalities, and small- to mid-sized businesses, IoT provides an opportunity to gain efficiencies, provides for greater automation, centralizes management of remote controllers, improves monitoring to predict or reduce failures, and reduces cost of running and maintaining systems and services. Along with all of these opportunities, though, come greater risks, especially when considering increased cyber attacks against connected devices that may result in physical disruption to services and systems.

The DHS National Cybersecurity and Communications Integration Center (NCCIC) is dedicated to assisting the Federal Government; State, local, Tribal, and territorial governments; and the private sector with cybersecurity concerns. This includes situational awareness, incident response, and information sharing related to IoT devices. The Industrial Control System Computer Emergency Readiness Team (ICS–CERT), housed within the NCCIC, focuses on and is closely monitoring the threats in IoT to industrial control systems. Recognizing that industrial control systems are both publicly and privately held, ICS–CERT has been providing a range of products and services to protect critical infrastructure in the context of threats in the Industrial Internet of Things.

DHS has invested in a pilot initiative by the DHS Science & Technology (S&T) Directorate to accelerate research and innovation around homeland security prior-

ities. S&T's first investment cycle on this initiative focuses on the IoT. This investment supports developing a solution that detects devices as they connect or disconnect from network infrastructure and sees how they communicate. It represents a solution for homeland security needs; in this case, securing networks that will eventually include sensitive oil pipelines, border monitoring assets, or airport screening systems. DHS S&T is also funding applied Research Development Test and Evaluation addressing Cyber-Physical Systems security in areas of Smart Manufacturing, Connected Automotive systems and Connected Medical Devices/Systems.

Cybersecurity requires an approach known as "defense in depth." There is no single technical solution that will effectively secure networks and computers, so companies and Government agencies have multiple layers of cybersecurity. While an adversary can break through any individual security layer, the intent of defense-in-depth is that an adversary will be detected or stopped before they can break through every single security layer. In the physical world, important information is not just protected by a locked door. Instead, important information may be in a safe, in a locked building, with guards, cameras, and a fence. This is the physical world's equivalent of defense-in-depth. As IoT makes connectivity more convenient, it also reinforces the need for defense in depth as a leading cybersecurity practice.

TRANSPORTATION SECURITY

Question 5a. In the past as well as this fiscal year, the funding for security for the surface transportation sector has been only a small fraction of the overall funding for the Transportation Security Administration's (TSA) mission. In fact, TSA spends only about 2 percent of its budget on surface transportation activities. At the same time, Transit Security Grants have been cut from a peak funding of $388 million to about $100 million, including Amtrak Grants.

Given that terrorists are increasingly focusing on soft targets, as well as the August 2015 attempted attack aboard a train traveling from Amsterdam to Paris, how concerned are you that the prioritization of aviation security over the surface sector could lead to vulnerabilities elsewhere?

Question 5b. Is the Federal Government doing enough to help secure our transit systems?

Answer. Securing surface transportation is very different from securing aviation. A primary characteristic of surface transportation systems is that these systems, in contrast to aviation systems, are more accessible and open given the need to accommodate high passenger and cargo volume. Unlike the aviation sector where TSA is responsible for operational security, and the accompanying costs, the primary responsibility for surface transportation security lies with the owners/operators of the systems. The percentage of funding that TSA allocates to surface initiatives is not indicative of a prioritization of aviation over surface transportation. Transportation entities costs are primarily shouldered by the system owners/operators, not the Federal Government. Additionally, over $2.4 billion in surface transportation security grant funds have been awarded since fiscal year 2006 for critical security initiatives.

TSA supports surface transportation stakeholders primarily through voluntary and collaborative programs. Using TSA's risk-based, intelligence-driven approach to security, TSA has developed a comprehensive, multi-layered program for security in the surface modes. Key layers in surface transportation programs include:

- *Information Sharing*.—Joint Terrorism Task Force (JTTF) partnerships, Homeland Security Information Network (HSIN) postings, Sector Coordinating Council (SCC) and the Government Coordinating Council (GCC) network, monthly calls with industry advisory groups, Security Awareness Messages, briefings through Field Intelligence Officers, Information Sharing and Analysis Centers' (ISAC) incident summaries, Transit and Rail Incident Awareness Daily (TRIAD) for industry stakeholders, and Daily Open Source Cyber Reports (distributed through the ISACs).
- *Grant Funding*.—TSA advises Federal Emergency Management Agency (FEMA) for DHS grants in the Transit Security Grant Program (TSGP), Intercity Passenger Rail Security Grant Program (Amtrak), and Intercity Bus Security Grant Program (IBSGP), and develops risk-based funding priorities on security initiatives in surface transportation. Grant funding has declined since its peak in fiscal year 2009, and recipients of these funds therefore focus mainly on maintaining and sustaining existing capabilities, including operational deterrence ("boots on the ground").
- *Drills and Exercises*.—TSA's Intermodal Security Training and Exercise Program (I–STEP) supports exercises which are regional in scope involving agency representation at the Federal, State, and local levels. A relatively new feature to the TSA exercise layer is a "Design-It-Yourself" exercise program named Ex-

ercise Information System (EXIS), which allows TSA to support individual agencies which design their own exercises on a smaller scale while using fewer resources than I–STEPs require.

- *Training*.—Each of TSA's subject-matter experts in the surface modes of transportation either has developed or is developing handbooks and guides containing important risk-reduction information for industry use. Through joint efforts with our industry stakeholders, DVDs and videos have been produced addressing such subjects as sabotage and potential threats in their operating environment. For example, the TSA First Observer™ program trains highway professionals to observe, assess, and report potential security and terrorism incidents.
- *Technical Assistance*.—This includes vulnerability assessments, guidance documents such as Security Information Bulletins, Lessons Learned, Recommended Practices, Protective Measures, the Security Measures and Resources Toolbox (SMARToolbox), Best Practices, and Standards.
- *Baseline Assessment for Security Enhancement (BASE)*.—TSA uses its Transportation Security Inspectors—Surface (TSI–S) to conduct BASE reviews on mass transit, passenger rail, and over-the-road bus systems. These reviews provide a comprehensive overview and evaluation of security programs in critical surface transportation systems across the country. The results of these assessments inform the development of risk mitigation priorities, security enhancement programs, and resource allocations, including funding priorities for the TSGP.
- *Visible Intermodal Prevention and Response (VIPR) teams*.—TSA deploys VIPR teams—consisting of teams of Federal Air Marshals, Behavior Detection Officers, Transportation Security Specialists—Explosives, Transportation Security Inspectors and Canine teams—across the United States, in close coordination with local security and law enforcement officials, to augment the security of transportation systems.

Through these programs, and others, TSA is efficiently utilizing available resources to ensure that surface transportation system owners and operators have the support and tools they need to raise and maintain their baseline levels of security.

Question 5c. Is there any indication that terrorists are targeting other transportation systems such as the Nation's rail system?

Question 5d. How would you assess the vulnerability of the Nation's transportation systems such as the Nations' rail system to attacks by home-grown terrorists?

Answer. TSA is not aware of any credible threat reporting against U.S. rail systems at this time, despite the FBI's recent arrest of a police officer with the Washington, DC, Metro Transit Police Department on charges of attempting to provide material support to a designated foreign terrorist organization. In fiscal year 2016, the Transportation Security Administration (TSA) conducted more than 2,400 Visible Intermodal Prevention and Response (VIPR) operations at mass transit, passenger rail, and freight rail locations in coordination with law enforcement and transportation system stakeholders. These VIPR operations mitigate terrorist risk by augmenting the security layers of these stakeholder partners. TSA's Office of Intelligence and Analysis made more than 300 intelligence engagements with freight rail and public transportation stakeholders (out of approximately 800 total engagements with all transportation stakeholders), including organizations such as the American Public Transportation Association and the Association of American Railroads. During these engagements, TSA intelligence analysts provided these stakeholders information about current tactics, techniques, and procedures used by terrorists in their attacks on these surface transportation modes world-wide. TSA uses a variety of information to provide this analysis, including intelligence and open-source reporting, and reviews of attacks against freight rail and public transportation systems.

Vulnerability of rail systems is very much dependent upon the particular location and operational purpose of the asset. TSA continues to engage with rail system operators to discuss the current threats and tradecraft being utilized by terrorists, as well as to collaboratively build a comprehensive, multi-layered program for securing these surface modes of transportation. On-going communication and information sharing among TSA and rail security coordinators and other stakeholders ensures existing vulnerabilities are actively mitigated and emerging threats are addressed. Many of the programs and resources already implemented and in place to support anti-terrorism activities also inherently address the risk of home-grown violent extremism.

Question 6a. Recently, the inspector general released a report detailing how certain 9/11 Act mandates have yet to be completed by TSA. Among these mandates

is are the issuance of regulations to assign risk tiers to carriers, as well as establishing front-line training requirements for employees.

When, in your estimation, will TSA issue guidance for these regulations to be finalized?

Answer. Completing the 9/11 Act regulatory requirements for surface transportation is, a priority for the TSA and DHS. The administrator of TSA has made his commitment to seeing these mandates through to completion in communications with both Congress and his staff. As noted below, TSA has a clear plan for ensuring it continues to make progress.

- *Security Training*.—As of July 12, 2016, a proposed rule to meet the security training requirements is with the Office of Management and Budget (OMB) for review and clearance to publish.
- *Vulnerability Assessments and Security Planning (VASP)*.—TSA intends to issue an Advance Notice of Proposed Rulemaking (ANPRM) to solicit sufficient data regarding the security measures industry currently employs as well as the potential impact of regulations on operations. This data is necessary to comply with minimum standards established by the OMB under Executive Order 12866, and related OMB guidance, which include conducting a robust analysis of the existing baseline of persons potentially affected by a proposed rule.
- *Employee Vetting*.—TSA intends to address the vetting requirements (threat assessment and immigration check) through a rulemaking to be published in sequence with the other surface security-related rulemakings (the rulemaking for security training will set the applicability and structure for all of the other related rulemakings). TSA has already satisfied the requirements of Sections 1414 and 1522 of the 9/11 Act, having published an Interim Final Rule on False Statements Regarding Security Background Checks (see 73 FR 44665) and issued various guidance documents (see, e.g., TSA's February 2007 updates to its recommended security action items for the highest-risk freight railroads, and background check practices published by the American Public Transportation Association in conjunction with TSA in 2011). TSA intends for all future rulemakings, including the surface employee vetting rule described above, to be consistent with the standards articulated in Sections 1414 and 1522.

There are a number of external factors impacting the development of regulations that are unpredictable and outside of the agency's control, therefore it is not possible to provide more detailed estimates for publications of these regulations at this time.

Question 6b. Please detail for us the changes you implemented regarding procedures for the workforce, technology, and standard operating procedures to the extent that you can in this setting.

Answer. The Transportation Security Administration (TSA) has implemented a number of steps to address the issues raised in 2015 by the Department of Homeland Security (DHS) Office of the Inspector General (OIG) covert testing. These steps include initiatives to ensure leadership accountability, improve alarm resolution, increase effectiveness and deterrence, increase threat testing to sharpen officer performance, strengthen operating procedures and technology, and enhance training. This included a root cause analysis that identified multiple areas for improvement, and TSA is mitigating those areas through program action plans. All of the actions I directed in the 10-Point Plan I gave to Administrator Neffenger are currently on-schedule or completed.

Question 7. Recent events have shown us that terrorists overseas continue to exploit security vulnerabilities to do harm to the commercial aviation sector. Last February, an aircraft originating from Mogadishu, Somalia was the target of an attempted attack. A terrorist was able to detonate a bomb concealed within a laptop, killing himself and injuring two others. Had the altitude been higher, the plane would have been destroyed. Last October, a flight originating from Sharm El Sheikh International Airport was destroyed midflight due to a reported bomb. Although not last points of departure to the United States, these attacks serve as reminders that we need to ensure that planes originating from foreign countries bound for the United States are as secure as possible. Please detail for us DHS and TSA's role in assessing last-point-of-departure airports and ensuring they meet all appropriate security standards.

Has the certification of Cuba as a last-point-of-departure airport differed from the process that is used for other last-point-of-departure airports?

Answer. The certification of Cuba's last-point-of-departure airports does not differ from the process that is used for other last-point-of-departure airports. Under Title 49 of the United States Code the Secretary of the Department of Homeland Security (DHS) is required to assess security at all foreign airports served by U.S. aircraft operators as well as at foreign airports serving as Last-Point-of-Departure (LPD) lo-

cations for foreign air carriers using the security standards adopted by the International Civil Aviation Organization (ICAO).

DHS has delegated responsibility for foreign airport security assessments to the Transportation Security Administration (TSA). DHS, particularly through its operational components and working closely with our United States Government interagency partners, plays a key role in the U.S.-Cuba relationship by securing flows of people between the United States and Cuba. In DHS headquarters, the Office of Policy assists the operators, like TSA and Customs and Border Protection, by providing coordination across the Department and with the Federal interagency partners, ensuring that the work of the components of the Department and their missions represent a unified effort.

Consistent with the regulations at 49 C.F.R. § 1544.3 and 1546.3, TSA evaluates the effectiveness of security measures maintained at foreign locations through assessments of foreign airports and inspections of air carriers that operate from those airports. To evaluate the security of the airports, TSA's Transportation Security Specialist use the Standards and Recommended Practices contained in Annex 17 to the Convention on International Civil Aviation adopted by ICAO. TSA conducts inspections of both U.S. and foreign airlines with direct service to the United States. These inspections are based on TSA-issued Standard Security Programs. The certification of Cuba's last-point-of-departure airports does not differ from the process that is used for other last-point-of-departure airports.

Question 8. In June 2015, the inspector general released a report detailing how aviation workers with links to terrorism were not vetted due to TSA not having access to certain watchlisting information. Earlier this year, we learned that TSA would receive the additional information to ensure that this does not happen again. Are you certain that TSA has all watchlisting information needed to thoroughly vet individuals in accordance with their responsibilities?

Answer. Following the June 2015 Inspector General report, the Transportation Security Administration (TSA), with the Department of Homeland Security, began receiving on an automated basis additional records in the Terrorist Identities Datamart Environment (TIDE). This information supplements TSA's current use of the Terrorist Screening Database (TSDB). In addition to containing records of individuals in the TSDB, TIDE provides information on individuals who have links to terrorists, terrorism, or terrorist activity, but who have not met the reasonable suspicion standard necessary to be nominated to the TSDB (the "Watch List"). Having automated access to this data makes it possible for TSA to make more informed Security Threat Assessment decisions for individuals seeking access to critical and sensitive transportation infrastructure.

TSA began automated receipt of non-U.S. citizen data at the end of February 2016 and in June 2016, the National Counterterrorism Center (NCTC) provided the first monthly manual transfer of U.S. citizen data. Following the completion of the ongoing technical changes across multiple agencies' systems necessary to support automated transfer of these records, TSA anticipates receiving the U.S. citizen data on an automated basis in late 2016.

Question 9. During the hearing, in response to a question from Representative Katko, you seemed to indicate that you were in agreement with the provision in his bill that would require an audit from the General Accountability Office before commercial air service could begin between Cuba and the United States. That would seem to be inconsistent with recent actions by the Department of Transportation, and your own Transportation Security Administration, to commence direct flights as soon as possible. Please clarify.

Answer. During the hearing it was unclear that Representative Katko suggested that the GAO review occur prior to commercial flights from Cuba. The assessments undertaken by TSA in conjunction with other Federal agencies are highly rigorous. We thoroughly respect the work of GAO, but do not agree that a GAO review prior to the commencement of scheduled commercial flights to Cuba is necessary or advisable.

Question 10. Is Federal Air Marshal presence a prerequisite for last-point-of-departure flights? To your knowledge, does an agreement for Federal Air Marshals exist for charter flights from Cuba to the United States currently, and if so, is such an agreement being pursued for scheduled flights?

Answer. The Federal Air Marshal Service (FAMS) is an important component of our multilayered aviation security but FAMS presence is not a prerequisite for last-point-of-departure flights. FAMs are deployed using a risk-based model.

My staff is available to discuss arrangements that have been mode with respect to FAMS presence on commercial flights to Cuba.

Question 11. Are you confident that TSA, DOT, and other agencies have been doing/are currently undertaking the due diligence necessary to ensure that scheduled travel from Cuba to the United States are secure?

Answer. Yes. TSA is coordinating with the Department of Transportation (DOT) and the Institute of Civil Aeronautics of Cuba (IACC) to ensure that security for forthcoming scheduled air service between our countries meets TSA's requirements as well as the high security expectations of the U.S. traveling public. For the past 5½ years, TSA and IACC have enjoyed a strong, professional relationship. During this period, IACC has responded favorably to the aviation security initiative proposed by TSA. DHS has conducted 37 airport assessments and air carrier inspections at Cuba's Last Point of Departure airports, with additional visits scheduled through the end of the calendar year. Through these assessments, DHS has determined that all of Cuba's airports serving the United States and all air carriers meet relevant international and United States security requirements.

SOCIAL MEDIA IN TRAVELER VETTING

Question 12a. Recently, U.S. Customs and Border Protection published a notice asking for public comment on the addition of a request for Visa Waiver Program travelers' social media identifiers as part of Electronic System for Travel Authorization (ESTA) applications and I–94W arrival and departure forms. The notice indicates that providing this information would be optional, and that collection this type of data "will enhance the existing investigative process" and "provide DHS greater clarity and visibility to possible nefarious activity and connections."

Can you please explain how this data will be used to enhance the screening of foreign travelers?

Answer. If an applicant chooses to answer this question, DHS will have timely visibility of the publicly-available information on those platforms, consistent with the privacy settings the applicant has set on the platforms. Highly-trained CBP personnel may review publicly available social media information as an additional data point to assist in CBP's vetting of an ESTA application. Information found in social media may be used to validate legitimate travel and to help identify potential threats. The information will not be used to prevent travel based on an applicant's political views, race, ethnicity, or religion.

Question 12b. How is DHS going to authenticate or confirm that the social media identifiers are truly associated with the person seeking to enter the United States?

Answer. CBP conducts thorough research of applicants and uses multiple tools to support positive identification of applicants in social media. Each case is reviewed individually and, after a careful review, a determination is made based on the totality of the circumstances.

Question 12c. Will these identifiers be protected in a similar way as other personally identifiable information?

Answer. Yes, social media identifiers will be safeguarded in the same manner as all other personally identifiable information (PII) collected through the Electronic System for Travel Authorization (ESTA) application. In addition, DHS will publish an updated Privacy Impact Assessment (PIA) and System of Record Notice (SORN) associated with enhancements to the ESTA application questionnaire, including the addition of an optional field for social media usernames or identifiers for all ESTA applicants.

VULNERABILITY OF "SOFT TARGETS"

Question 13. The tragic mass shooting in Orlando and the sophisticated, coordinated attacks at the airport in Istanbul remind us how vulnerable soft targets often are. How do your agencies coordinate to ensure that owners and operators of sports stadiums, movie theaters, schools, and other soft targets have the information and guidance they need to secure their facilities?

Answer. The National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) serves as the Sector-Specific Agency (SSA) of the Commercial Facilities Sector, one of 16 critical infrastructure sectors, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within this sector operate on the principle of open public access, meaning that the general public can move freely without the deterrent of highly visible security barriers. Since its inception, in its role as SSA for the Commercial Facilities Sector, IP has aggressively coordinated with these private-sector owners and operators, both during an incident and steady-state operations.

During times of targeted threat or heightened security posture, or when there are issues necessitating a private-sector perspective, IP follows its "Coordination Plan for Targeted Threat and Security Engagements." The plan, which is implemented

for both Classified and Unclassified engagements, facilitates the rapid convening of private-sector partners and other critical infrastructure stakeholders. This capability aims to advance IP's ability to share Classified information remotely, as opposed to only convening meetings in the National Capital Region.

During domestic incidents such as the events in Orlando, or following foreign attacks such as those in Paris, IP, in coordination with the Office of Intelligence & Analysis and frequently the Federal Bureau of Investigation, also rapidly convenes its sector and other State, local, Tribal, and territorial partners for information-sharing calls at the FOUO level. These calls consist of a threat briefing, a status update, suggested protective measures, and an open forum discussion for partners to provide a quick, comprehensive snapshot of their sector or industries' activities.

During steady state, IP works with partners on a number of programs that educate the Commercial Facilities Sector partnership base, stakeholders, and the general public on suspicious behavior, protective measures, and risk mitigation. Broad programs include the "If You See Something, Say Something™" campaign, the "Hometown Security" campaign, and the Active Shooter Preparedness Program. In addition, IP has produced and distributed a number of other resources, including:

- Suspicious Activity training videos;
- On-line Training Courses (Active Shooter, Surveillance Awareness, Insider Threat);
- Protective Measures Guides; and;
- Specialized guides (Evacuation Planning, Patron Screening, Bag Search).

In addition, the Interagency Security Committee (ISC) released *Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide* as an FOUO document in July 2015. The publication is divided into two parts: First, a new policy requirement for all nonmilitary Federal facilities within the Executive branch of the Government; second, a set of best practices and recommendations (not policy requirements) to assist with implementing the active-shooter policy. The ISC published a non-FOUO version of the same document in November 2015 to ensure availability and visibility by a much broader audience.

USE OF SOCIAL MEDIA

Question 14a. We have heard a lot in recent months about how to enhance and even codify Federal efforts to scrutinize the social media activity of suspected terrorists. Recently, several of my colleagues and I hosted a forum on the threat of domestic anti-Government groups. We heard testimony from advocates like the Southern Poverty Law Center and others, that domestic terrorist organizations are recruiting and spreading their message in much the same way as ISIS—through internet forums and social media campaigns.

How are the agencies you represent monitoring the on-line activities of domestic terror groups?

Answer. DHS does not provide constant monitoring of on-line activities; However, should there be a validated collection requirement targeting specific information about a domestic terrorist organization, relevant DHS components would target this organization for collection. This would include periodic reviews of publically-available information related to the organization for the purpose of answering the targeted collection requirement until that requirement expires or is cancelled by the organization requesting the collection.

Question 14b. Are your methods different from those used to screen for individuals who may be influenced by foreign, overseas terrorist organizations?

Answer. Social media can provide the Department with critical information related to the execution of our mission. The Department uses social media in a number of ways, both foreign and domestic, which we have expanded in recent years. Today, social media is used for over 30 different operational or investigative purposes by U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, Transportation Security Administration, Federal Emergency Management Agency, other DHS components and offices. Operational uses are consistent with Departmental authorities and included research, watch and warning, screening and vetting, investigations and personnel security.

QUESTIONS FROM HONORABLE LORETTA SANCHEZ FOR HONORABLE JEH C. JOHNSON

Question 1a. Thank you Mr. Chairman, and thank you for joining us, Secretary Johnson and Directors Rasmussen and Comey. Secretary Johnson, in March you came before our committee and we discussed the Countering Violent Extremism mission. I am happy to see that since then the Department of Homeland Security noticed the new Countering Violent Extremism Grant Program to loop in non-profits

and community organizations in the fight against terror. I agree with the notion that we should have a local community-based component to our CVE mission, and I think this will compliment your great work in finding innovative ways to address the evolving threat environment.

As we continue to see efforts to break down informational silos across the State and Federal level, will there be greater opportunity for information sharing between State and Federal partners?

Question 1b. Will there be more information sharing with State fusion centers regarding high-level threat actors and operations?

Answer. The U.S. Department of Homeland Security (DHS) takes very seriously our mission to equip the Homeland Security Enterprise (HSE), which includes State, local, Tribal, territorial (SLTT) and private-sector partners, with timely intelligence and information sharing. At DHS, the Office of Intelligence and Analysis (I&A) is the intelligence community element statutorily charged with delivering intelligence to SLTT and private-sector partners, and also sharing information from those partners with the Department and the IC. As such, I&A is responsible for ensuring SLTT and private-sector partners can expeditiously access the capabilities, resources, and expertise of the Department and serve as full participants in the HSE. I&A deploys 100 personnel to State and major urban area fusion centers and other strategic locations Nation-wide in support of SLTT and private-sector partners. The mission of I&A field personnel is to engage SLTT and private-sector partners to facilitate the intelligence cycle at the local level by: (1) Building relationships and providing intelligence and information-sharing support, (2) conducting intelligence collections and reporting, and (3) producing intelligence analytic products.

I&A integrates information collected every day across DHS and from our SLTT partners into our analysis. We continue to make progress and aggressively work to overcome barriers to information sharing as we bring SLTT information into the IC, and share IC information with our SLTT and private-sector partners. In 2015, we launched the Field Analysis Report (FAR), a new analytical product that incorporates views and assessments from SLTT partners to provide local, State-wide, and regional perspective to National strategic intelligence issues.

In addition, our new data cloud initiative, the DHS Data Framework, is pulling in the most critical data sets of the Department to enhance data sharing across the DHS Intelligence Enterprise and fill critical gaps across the IC and with our SLTT and private-sector partners. At the same time, we continue to deepen our relationships with our SLTT and private-sector partners through our support of the National Network of Fusion Centers with personnel, training, Federal grants, security clearances, and Classified systems access, which allow DHS to better share information regarding threats. DHS is actively executing an information-sharing environment where Federal, SLTT, and private-sector partners can seamlessly share and access information, with appropriate protections, in real time.

Question 1c. If a State wants to enforce a higher level of cybersecurity standards than those that are adopted at the Federal level, is DHS committed to supporting such efforts?

Answer. Yes. While the Department of Homeland Security leads a National effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure, individual States are in the position to select a risk posture that best suits the State, and use tailored cybersecurity programs, with support from the Federal level.

One resource States use is the National Institute of Standards and Technology Cybersecurity Framework, the current guidance document for cybersecurity best practices. As codified under Executive Order 13636, DHS supports and promotes use of the Cybersecurity Framework a flexible tool adaptable to unique circumstances, recognizing that the majority of threat actors can be stopped by implementation of best practices in cybersecurity. As a supplementary resource, in DHS's voluntary Nation-wide Cyber Security Review, the questions for consideration align to the Framework. The Framework uses international-recognized consensus-based standards, and we would encourage States to build their policies on similar globally-accepted standards and practices.

DHS supports a range of efforts by States to increase cybersecurity preparedness, but recognizes that limited resources can be an issue. To address State resourcing, FEMA provides State and local governments with preparedness program funding in the form of Non-Disaster Grants to build, sustain, and deliver core capabilities essential to achieving the National Preparedness Goal of a secure and resilient Nation. The building, sustainment, and delivery of these core capabilities requires the combined effort of the whole community, rather than the exclusive effort of any single organization or level of government. States are encouraged to include cybersecu-

rity preparedness into their decisions when determining best use of this grant money.

Additionally, to support the cyber workforce at the State level, the Scholarship for Service program is designed to increase and strengthen the cybersecurity workforce that protects the Government's critical information infrastructure. The program provides scholarships for college and graduate students studying cybersecurity. These scholarships are now eligible for service agreements in not only Federal service, but in State, local, or Tribal government organizations; yet the program is Federally-funded.

Question 2. As new transit modes such as the California High Speed Rail or the Orange County Streetcar come on-line what steps should agencies take or what guidance should they follow to ensure the supporting systems are safe from cyber attack?

Answer. To better support SLTT work and provide technical expertise and outreach, DHS provides four primary initiatives: Funding the MS–ISAC, offering voluntary risk assessments, holding cybersecurity exercises, and offering incident response assistance. The MS–ISAC is the DHS-designated Information Sharing and Analysis Center (ISAC) for all SLTT governments. The MS–ISAC supports SLTT governments by providing education and awareness, a 24×7 security operations center, and technical expertise in malware analysis, forensic analysis, and incident response/mitigation. The MS–ISAC acts as a force-multiplier for DHS in reaching out to the tens of thousands of SLTT governments across the country. These activities may be relevant to mass public transit lines as well.

Moreover, DHS' NCCIC shares information among public and private-sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost. These resources can be found at: *https://www.us-cert.gov/ncas* and *https://ics-cert.us-cert.gov/*. Additionally, we encourage critical infrastructure owners and operators, such as public transportation operators in question, to adopt best practices by implementing the Cybersecurity Framework. Industry-led information-sharing analysis organizations or centers (ISAOs/ISACs) can be a powerful resource for industry-specific information sharing and best practices.

Question 3. I have spoken with the Orange County Transit Authority, which is located in my district. OCTA and other nearby public agencies that support critical infrastructure are constantly under cyber attack and they want to know what they can do to provide meaningful attack information to fusion centers or other law enforcement that will help reduce the overall cyber threat?

Answer. Agencies such as Orange County Transit Authority (OCTA) have a number of options available to reduce cyber risk. To help transit agencies better understand and utilize services provided by the Department of Homeland Security, the Department is deploying Cyber Security Advisors (CSA) across the country. A CSA is currently assigned to the Los Angeles/Orange County area. OCTA and other local government partners can reach out to cyberadvisor@hq.dhs.gov to be connected to their local CSA. For example, one key area where CSAs can assist is to increase organizations' ability to prepare for disruptions and successfully manage them should they occur. DHS's CSAs can help organizations build these kinds of capabilities by providing resources like the Cyber Resilience Review, among others.

Information sharing is a key part of the Department of Homeland Security's mission to create shared situational awareness of malicious cyber activity. DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24×7 cyber situational awareness, incident response, and management center that is a National nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. As provided by the Cybersecurity Act of 2015 (Pub. L. 114–113, Division N), DHS serves as the Government's central hub for automated cyber threat indicator sharing. By participating in the Automated Indicator Sharing (AIS) initiative, organizations receive machine-readable cyber threat indicators to immediately detect and block cybersecurity threats.

An entity that is a victim of a cyber incident can receive assistance from Federal agencies, which are prepared to investigate an incident, mitigate its consequences, and help prevent future incidents. For example, Federal law enforcement agencies have highly-trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other Federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and

capabilities both to minimize asset vulnerability and bring malicious actors to justice.

Entities experiencing cyber incidents are encouraged to report a cyber incident to the National Cybersecurity and Communications Integration Center. local field offices of Federal law enforcement agencies, their sector-specific agency, or any of the Federal agencies including the Federal Bureau of Investigation (FBI), the National Cyber Investigative Joint Task Force, the United States Secret Service, or United States Immigration and Customs Enforcement Homeland Security Investigations. The Federal agency receiving the initial report will coordinate with other relevant Federal stakeholders in responding to the incident.

Question 4. There are numerous public and private resources that provide information on cyber threats. What should smaller to mid-size agencies do to filter out the noise and focus on actionable information?

Answer. DHS is working to promote a strong cyber ecosystem that will shape the information technology market so that systems are more secure, to include researching vulnerabilities, driving developers to implement best practices, and developing standards to foster a market for interoperable security products that will enable small and medium agencies to better secure themselves. DHS also provides threat intelligence products tailored to the needs of Federal network defenders to identify the most significant threats. To help State, local, Tribal, and territorial (SLTT) governments, DHS has created a packet of resources specially designed to help them recognize and address their cybersecurity risks. These resources have been aligned to the five Cybersecurity Framework Function Areas. Additional information can be found at: *https://www.us-cert.gov/ccubedvp/sltt.* In addition to aligning activities to the Cybersecurity Framework, and subscribing to alerts published by the Department of Homeland Security, State government agencies may choose to participate in the DHS-funded Multi-State Information Sharing and Analysis Center (MS–ISAC) for cyber threat prevention, protection, response, and recovery information targeted to the SLTT governments.