WORLDWIDE THREATS AND HOMELAND SECURITY CHALLENGES

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

OCTOBER 21, 2015

Serial No. 114–37

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

99–743 PDF WASHINGTON : 2016

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

COMMITTEE ON 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 AND HOMELAND SECURITY CHALLENGES

Wednesday, October 21, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
New York, NY.

The committee met, pursuant to call, at 10:12 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, Barletta, Perry, Clawson, Katko, Hurd, Carter, Walker, Loudermilk, McSally, Ratcliffe, Donovan, Thompson, Jackson Lee, Langevin, Richmond, Keating, Vela, Watson Coleman, Rice, and Torres.

Chairman MCCAUL. The Committee on Homeland Security will come to order. The committee is meeting today to examine current and evolving threats to the homeland. I now recognize myself for an opening statement.

First, I would like to thank our witnesses for joining us here today and for offering their insights on the security challenges that we face at home and abroad.

We will cover a lot of ground today from America's border security to our cyber defenses, but I want to focus, in particular, on the rising terror threat to the homeland.

Last month, this committee held the first-ever Congressional hearing at the 9/11 Memorial Museum in New York. On hallowed ground, we were reminded of the solemn pledge our country made in the aftermath to never let such a day happen again.

That resolve became the rallying cry of this Nation as we embarked on a generational war against Islamist terror. Fourteen years later, we are still engaged in that struggle. Today, I expect an unvarnished assessment from our witnesses about where we stand in the fight.

We are at a turning point in the new age of terror. I predict this year could exceed the last to become the most violent year on record for global terrorism. Radical Islamists are recruiting on-line across borders and at broadband speed, and the impact is being felt world-wide. Here in the United States, there have been more terrorist cases this year involving home-grown Jihadists than any full year since 9/11. ISIS alone has inspired, or directed, 17 terror plots in America since early 2014, and overall, the group has been linked to more than 60 plots against Western targets from Canada to Australia. The pace of terror plotting is unprecedented, unrivaled, even by al-Qaeda at its peak. Yet, we are no closer to dismantling ISIS

than we were a year ago. Despite 14 months of air strikes, the group has largely maintained its core safe haven while expanding its global footprint. The ISIS reign of terror is fueled by its recruitment of foreign fighters who hail from more than 100 countries, including our own.

This committee launched a bipartisan task force to examine the foreign fighter threat, and last month, the group released its final report with some very disturbing findings. Overall, they found that we are losing the struggle to stop Americans from traveling overseas to join jihadists. We have managed—only managed to stop a small fraction of the hundreds of Americans who have attempted to fight in Syria and Iraq, and some have even managed to make it back into the United States after enlisting with terrorist groups.

We are falling behind the threat for many reasons. Vulnerable young people are being recruited at record speeds, and terrorists are shifting their communications to Dark Space, which has made it far more difficult to monitor and intercept suspects. These secured communication tools are also being used to plot attacks in our own country.

Moreover, gaping security weaknesses overseas, especially in Europe, are making it easier for extremists to travel to and from the conflict zone. But at the end of the day, we cannot keep individuals from being lured to terrorist hotspots unless we eliminate the problem at its source. Sadly, those prospects have grown darker.

The President's failure to develop a coherent strategy in Syria and Iraq has emboldened our adversaries to fill the vacuum with disastrous consequences. Russia and Iran are now propping up Assad, and there are reports that even Cuban special forces have joined the fight. Those rogue regimes will fan the flames of sectarianism and make it harder for us to eliminate the terrorist sanctuary in the region. Their actions will also intensify refugee flows, which have become a serious security challenge in light of reports that terrorists are exploiting the crisis to sneak operatives into the West.

Violent extremists are also expanding their foothold from Libya to Afghanistan. Yet, I am alarmed that we lack a clear vision for reversing their gains and winning the wider war against Islamist terror. If we fail to defeat our enemies overseas and combat them in their hateful ideology, we will be forced to fight more of them here at home. We have learned this the hard way. Today, I hope to hear from our witnesses about these challenges and how their agencies are working to strengthen our defenses on the home front.

Again, I want to express my gratitude to each of you for your close and continued cooperation with this committee, your dedication to our country, and your success this year in disrupting so many terrorist plots.

Let me just close by saying that the FBI and Homeland working together have arrested almost 70 ISIS-related individuals in this country. I am amazed at what we have been able to stop, and I just want to commend you for that.

With that, the Chair recognizes the Ranking Member.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

OCTOBER 21, 2015

Good morning. I'd like to thank our witnesses for joining us and for offering their insights on the security challenges we face at home and abroad. We will cover a lot of ground today—from America's border security to our cyber defenses—but I want to focus in particular on the rising terror threat to the homeland.

Last month, this committee held the first-ever Congressional hearing at the 9/11 Memorial Museum in New York. And on hallowed ground, we were reminded of the solemn pledge our country made in the aftermath: To never let such a day happen again. That resolve became the rallying cry of this Nation as we embarked on a generational war against Islamist terror.

Fourteen years later, we are still engaged in that struggle, and today I expect an unvarnished assessment from our witnesses about where we stand in the fight.

We are at a turning point in a new age of terror. I predict this year could exceed the last to become the most violent year on record for global terrorism. Radical Islamists are recruiting on-line, across borders, and at broadband speed—and the impact is being felt world-wide. Here in the United States, there have been more terrorist cases this year involving home-grown jihadists than any full year since 9/11.

ISIS alone has inspired or directed 17 terrorist plots in America since early 2014, and overall the group has been linked to more than 60 plots against Western targets, from Canada to Australia. This pace of terror plotting is unprecedented—unrivaled even by al-Qaeda at its peak. Yet we are no closer to dismantling ISIS than we were a year ago.

Despite 14 months of airstrikes, the group has largely maintained its core safe haven while expanding its global footprint. The ISIS reign of terror is fueled by its recruitment of foreign fighters, who hail from more than 100 countries, including our own.

This committee launched a bipartisan task force to examine the foreign fighter threat, and last month the group released its final report with some very disturbing findings. Overall, they found that we are losing the struggle to stop Americans from traveling overseas to join jihadists.

We have only managed to stop a small fraction of the hundreds of Americans who have attempted to fight in Syria and Iraq, and some have even managed to make it back into the United States after enlisting with terrorist groups. We are falling behind the threat for many reasons.

Vulnerable young people are being recruited at record speeds, and terrorists are shifting their communications to "dark space," which has made it far more difficult to monitor and intercept suspects. These secure communication tools are also being used to plot attacks in our country.

Moreover, gaping security weaknesses overseas—especially in Europe—are making it easier for extremists to travel to and from the conflict zone. But at the end of the day, we cannot keep individuals from being lured to terrorist hotspots unless we eliminate the problem at the source.

Sadly, those prospects have grown darker. The President's failure to develop a coherent strategy in Syria and Iraq has emboldened our adversaries to fill the vacuum, with disastrous consequences.

Russia and Iran are now propping up Assad, and there are reports that even Cuban special forces have joined the fight. These rogue regimes will fan the flames of sectarianism and make it harder for us to eliminate the terrorist sanctuary in the region. Their actions will also intensify refugee flows, which have become a serious security challenge in light of reports that terrorists are exploiting the crisis to sneak operatives into the West.

Violent extremists are also expanding their foothold from Libya to Afghanistan, yet I am alarmed that we lack a clear vision for reversing their gains and winning the wider war against Islamist terror. If we fail to defeat our enemies overseas and combat their hateful ideology, we will be forced to fight more of them here at home. We have learned this the hard way.

Today I hope to hear from our witnesses about these challenges and how their agencies are working to strengthen our defenses on the home front.

I want to express my gratitude to each of you for your close and continuing cooperation with this committee, your dedication to country, and your successes this year in disrupting terrorist threats against the American people.

Mr. THOMPSON. I thank the Chairman for holding today's hearing.

Mr. Secretary, welcome to what is your first appearance before this committee, this Congress. I look forward to hearing your informed perspective on today's topic.

I would also like to thank Director Rasmussen and Director Comey for their testimonies.

Mr. Chairman, while I agree that the threats to this Nation are concerning and worthy of examination, I also believe that as the authorizing committee of the Department of Homeland Security, it is our responsibility to hear from the Secretary about the overall management of DHS.

This bipartisan committee, the Government Accountability Office and the inspector general, have all identified challenges within the Department. Additionally, there are components within the Department that have proposed restructuring. While the Secretary's Unity of Effort initiative has made strides since the beginning of the Congress, but the Federal employee viewpoint survey still indicates that DHS has a long way to go in improving workforce morale, also to DHS components with a zero-fail mission, the Transportation Security Administration and the Secret Service are on-going much-needed reform.

Furthermore, the Department's cyber mission is critical as we look to prevent crippling attacks from cyber terrorists. While we have heard from several DHS officials, this Congress, we have yet to hear from the head of the agency on the record about how he is fulfilling his vision for the Department and what he needs from Congress.

Today's hearing and the topic and testimony does not provide for a hearing from the Secretary on the topics I have mentioned. Therefore, I am asking you, Mr. Chairman, for a commitment at some point to hold a hearing on the oversight of the Department of Homeland Security and invite Secretary Johnson to testify before the end of the first session of Congress. I know the success of the Department is a shared concern. Each Member of this committee should have the opportunity to question the Secretary in an open setting and to continue to hold him accountable.

Today's hearing on the world-wide threats gives the committee the opportunity to hear the perspective of top Government officials on the wide-ranging threat of terrorism from both international groups and domestic terrorists. Through its oversight, this committee has given attention to the threat from international terror organizations, including al-Qaeda and the Arabian Peninsula and the threat from Islamic State of Iraq and Levant.

The committee's bipartisan task force looked at the threat from foreign fighters, and one of their glaring, yet unsurprising findings, is that there are still intelligence and information-sharing gaps that need to be addressed. These gaps also enter the conversation as we continue our efforts to address our humanitarian response to the refugee crisis in Syria. I want to hear from each witness about their agency's intelligence capability and how they are working together as we prepare to assist in this humanitarian crisis.

As Members of Congress, we have the responsibility to convey accurate information to our constituents and to the media. As we rightfully continue to address the threats from international terrorist organizations, I want to reemphasize that we should not lose

sight of the threats posed by terrorists that are right here in America, as they are those that have no plans on traveling overseas to receive training from any international group. Through social media networks, ISIL has encouraged lone offenders to perpetrate violence right here on our soil. This approach is not novel. Right-winged domestic terrorist groups also use social media to recruit and communicate.

Again, Mr. Chairman, violent extremists view no single ideology or recruitment tactic, even though some Federal officials have been dismissive of domestic terrorism, and others generate false intelligence to the contrary. The facts are clear: Since September 11, more people in the United States have died in attacks by domestic extremists than in attacks by international terrorist groups.

Mr. Chairman, we often discuss what the 9/11 Commissioners call a failure of imagination. As we use today to discuss the threats to our country, let us not fail to imagine the devastation that can be caused by the extremists, both abroad and in our backyards. With that, Mr. Chairman, I yield back my time.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

While I agree that the threats to this Nation are of concern and should be examined, I also believe that as the authorizing Committee of the Department of Homeland Security, it is our responsibility to hear from the Secretary about the overall management of DHS. This committee, through its bipartisan work, the Government Accountability Office, and the Inspector General have all identified challenges within the Department.

Additionally, there are components within the Department that have proposed restructuring, the Secretary's Unity of Effort initiative has made strides since the beginning of the Congress, and the Federal Employee Viewpoint Survey still indicates that DHS has a long way to go in improving the morale of its workforce.

Furthermore, two DHS components with a zero-fail mission—the Transportation Security Administration and the Secret Service—are undergoing much-needed reform, and the Department's cyber mission is critical as we look to prevent crippling attacks from cyber terrorists abroad. While we have heard from several DHS officials this Congress, we have yet to hear from the head of the agency on the record about how he is fulfilling his vision for the Department and what he needs from Congress.

Today's hearing topic and testimony does not provide for hearing from the Secretary on the topics I have mentioned. Therefore, I am asking you for a commitment to hold a hearing on the oversight of the Department of Homeland Security and invite Secretary Johnson to testify before the end of the first session of this Congress. I know the success of the Department of Homeland Security is a shared concern. Each Member of this committee should have the opportunity to question the Secretary in an open setting and to continue to hold him accountable.

Today's hearing on world-wide threats gives the committee the opportunity to hear the perspective of top Government officials on the wide-ranging threat of terrorism from both international groups and domestic terrorists. Through its oversight, this committee has given much-needed attention to the threat international terror organizations including al-Qaeda in the Arabian Peninsula and the threat from the Islamic State of Iraq and the Levant.

The committee's bipartisan task force looked at the threat from foreign fighters and one of their glaring, yet unsurprising findings is that there are still intelligence and information-sharing gaps that need to be addressed. Those gaps also enter the conversation as we continue our efforts to address our humanitarian response to the refugee crisis in Syria.

I want to hear from each of the witnesses more about their agencies' intelligence capabilities and how the interagency is working together as we prepare to assist in this humanitarian crisis. As Members of Congress, we have a responsibility to have accurate information before we begin to spread our own propaganda to our constituents and to the media. As we rightfully continue to address the threats from international terrorist organizations, I want to reemphasize that we should not lose sight

of the threats posed by terrorists that are right here in America. There are those that have no plans on traveling overseas to receive training from any international group.

Through social media networks, ISIL has encouraged lone offenders to perpetrate violence right here on our soil. This approach is not novel. Not only does ISIL use social media to encourage lone offenders, but right-wing domestic terror groups also use social media to recruit and communicate. Once again illustrating that violent extremist views know no single ideology and recruitment tactics can mirror.

Even though some Federal officials have been dismissive of domestic terrorism and others generate false intelligence to the contrary, the facts are clear—since September 11, more people in the United States have died in attacks by domestic extremists than attacks associated with international terrorist groups. According to a survey conducted by the Police Executive Research Forum and the Triangle Center on Terrorism and Homeland Security, law enforcement places threats from right-wing terrorists as one of the top three terror threats in their jurisdiction.

We often discuss what the 9/11 Commissioners called failure of imagination. As we use today to discuss the threats to our country, let us not fail to imagine the devastation that can be caused by extremists both abroad and in our back yards.

Chairman MCCAUL. I thank the Ranking Member. I appreciate your bipartisan cooperation on the task force report, which I think was valuable, and hopefully to Federal law enforcement in the intelligence community. I will honor your request to have another hearing on the oversight issue as well.

We have a distinguished panel before us. First, the Honorable Jeh Johnson, who has served as the fourth Secretary of Homeland Security since his swearing in on December 23, 2013. Previously, he served as the general counsel for the Department of Defense where he led over 10,000 civilian and military lawyers across the Department and worked on the raid operation on the compound in Abbottabad to take down Osama bin Laden.

Next, the Honorable Nicholas Rasmussen has served as a director for the National Counterterrorism Center since December 2014, served as the deputy director, and is a member of the National Security Council staff where he was special assistant to the President, and senior director for counterterrorism.

Finally, we have the Honorable James Comey, who has served as the Federal Bureau of Investigation's director since September 2013. Previously, he was general counsel for Bridgewater Associates, and deputy attorney general at the Department of Justice. He also worked on the Exile program, which I remember meeting with you, sir, a long time ago when I was deputy attorney general for the State of Texas trying to implement the same program in the State of Texas, and we thank you for being here as well.

Witnesses' full written statements will appear in the record. I will remind Members that additional statements may be submitted for the record.

[The statement of Hon. Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

OCTOBER 21, 2015

Chairman McCaul and Ranking Member Thompson, thank you for this opportunity to hear testimony on "World-wide Threats and Homeland Security Challenges."

I join my colleagues on the committee in welcoming the Secretary of Homeland Security Jeh Johnson, FBI director James Comey, 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, and Homeland Secu-

rity the topic of threats to homeland security is of has significance in light of the events over the last 12 months.

My primary domestic security concerns are:

- to preventing foreign fighters and foreign-trained fighters from entering the United States undetected;
- countering violent extremism in the United States that is domestic and international in nature;
- 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

It is estimated that 250 U.S. citizens are among the number of foreign recruits who have traveled to Syria since the beginning of the conflict.

In 2014 the total number of foreign fighters entering Syria was estimated to be 14,000.

A September 26, 2015 article in the *New York Times* has the number of foreign fighters as 30,000, which is doubled the number of foreign recruits of a year ago.

It is estimated that since 2011 foreign fighters have come from over 100 countries.

This disturbing news coupled with the massive migration of people seeking to flee from war-torn Syria now entering Europe by the thousands raises important concerns regarding security.

The Obama administration has announced that the United States would take in 10,000 refugees by working the High Commissioner on Refugees in a long and structured vetting process.

The larger issue is not the process managed by the State Department and the Department of Health and Human Services that has long ago proven itself effective in identifying refugees who will be welcomed guests in the United States.

Every year, the United States provides resettlement opportunities to thousands of the world's most vulnerable refugees, in a program endorsed by the President (and every President since 1980) through an annual determination.

The U.S. Refugee Admissions Program (USRAP), which resettled over 58,000 refugees in the United States in 2012, reflects our own tradition as a Nation of immigrants and refugees.

I have long advocated for the plight of women and children in the Syrian war, who now make up a significant percentage of those escaping into Europe.

To qualify for refugee resettlement to the United States, refugees must:

1. Be among those refugees determined by the President to be of special humanitarian concern to the United States;
2. Meet the definition of a refugee pursuant to Section 101(a)(42) of the INA (see below);
3. Not be firmly resettled in any third country; and
4. Be otherwise admissible under U.S. law.

The application process for admittance into the United States as refugees is not easy nor is it quick.

The unprecedented circumstances that Europe is facing does mean that the United States must exercise diligence in every step of the process that will be followed that will allow up to 10,000 refugees from the Syrian war into the United States.

Countering Violent Extremism

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 of the acts that are intended to intimidate or terrorize the public.

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.

A domestic terrorist differs from a home-grown violent extremist in that the former is not inspired by, and does not take direction from, a foreign terrorist group or other foreign power.

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.

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 event when they are unpopular is not a crime.

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

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 several African American Churches have fallen victim to fires.

Historically, African American churches are the center of religious, social, cultural, and political life for the communities they serve.

Because of their importance to the social movements of the 1960s in less than one month in 1962, 5 Black churches were burned in the State of Georgia.

Securing Critical Infrastructure

Last week 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.

For example, the bill lays the foundation for the development of tools to create enhanced computer modeling capabilities to determine potential impacts on critical infrastructure under various incident and threat scenarios as well as the potential for cascading failures that impact other critical infrastructure should certain critical infrastructure(s) be impacted by a terrorists attack or an All Hazards event.

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.

The arrival of the Internet of Things, which will introduce ubiquitous wireless technology that will have significant implications for existing computing networks and their security.

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

It is the work of the committee to ensure that the Department of Homeland Security has what it needs to meet the cybersecurity challenges that it faces.

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 World-wide Threats and Homeland Security Challenges.

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

Chairman MCCAUL. The Chair now recognizes Secretary Johnson for an opening statement.

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

Secretary JOHNSON. Thank you, Chairman, Congressman Thompson, Members of the committee. It is a pleasure to appear before you again. You have my prepared statement. I will not read it in its entirety. Let me just give you a few thoughts.

Last month, I attended, on 9/11, the ceremony that occurred in Shanksville, Pennsylvania. This was the 14th anniversary of 9/11. That ceremony, in particular, was a sobering reminder of the acts of terrorism, but also the acts of heroism that day, particularly on Flight 93, the 40 passengers and crew that day. I met almost all of their families that day.

The events on 9/11 were the most prominent and devastating example of terrorist attacks by those who are recruited, trained, and directed overseas and exported to our homeland. The 9/11 hijackers were acting on orders from al-Qaeda's external operations chief, Khalid Sheikh Mohammed, who was, in turn, carrying out the direction of Osama bin Laden. Likewise, the attempted Shoe Bomber in December 2001, the attempted Underwear Bomber in December 2009, the attempted Times Square car bombing in May 2010, and the attempted package bomb plot in October 2010 were all efforts to export terrorism to the United States, and they all appeared to have been directed by terrorist organizations overseas.

The response to these types of attacks and attempted attacks on our homeland was and is to take the fight directly to the terrorist organizations at locations overseas. But today, the global terrorist threat is more decentralized, more complex, and, in many respects, harder to detect.

The new reality involves the potential for smaller-scale attacks by those who are either home-grown or home-based, not exported, and who are inspired by, but not necessarily directed by, a terrorist organization.

Today, it is no longer necessary for terrorist organizations to personally recruit, train, and direct operatives overseas and in secret and export them to the United States to commit a terrorist attack.

Today, with new and skilled use of the internet, terrorist organizations may publicly recruit and inspire individuals to conduct attacks within their own homelands.

Al-Qaeda in the Arabian Peninsula no longer hides the fact that it builds bombs. It publicizes its instruction manual and its magazine, and publicly urges people to use it.

Today, we are also concerned about foreign terrorist fighters who are answering public calls to leave their home countries in Europe and elsewhere to travel to Iraq and Syria, and to take up the extremist fight there. Many of these individuals will return to their home countries with an extremist motive. In this regard, I compliment this committee for the report it issued on September 29 concerning foreign terrorist fighters. I have read it. I believe this committee's work is spot on, in many respects, in your assessments of the risk.

As noted in the report, my Department has undertaken much of what is recommended. We have been, and are continuing to institute measures to detect and prevent travel by foreign terrorist fighters, along with the good work of the FBI.

The recent wave of attacks and attempted attacks here and in Europe reflect the new reality of the global terrorist threat: The Boston Marathon Bombing in April 2013; the attack on the war memorial and the parliament building in Ottawa in October 2014; the attack on the Charlie Hebdo Headquarters in Paris, France in January 2015; the attempted attack in Garland City, Texas in May 2015; and the attack that killed five U.S. service members in Chattanooga, Tennessee, in July.

What do these wave of attacks, recent attacks, and attempted attacks, all have in common? They were all conducted by home-grown or home-based actors, and they all appear to have been inspired but not directed by al-Qaeda or ISIL.

Finally, we are concerned about domestic terrorism in the form of a lone wolf who can include various aspects—which can include various aspects of domestic terrorism, such as right-wing extremism. We need to devote substantial efforts to the study and understanding of these threats and will continue to further our understanding of the underpinning of terrorist threats in all forms.

In terms of what we are doing about it, I look forward to your questions.

The last two thoughts I have: Members of Congress ask me, what can we do to help? How can we support the Department's homeland security missions? There are two things I would like to leave

you with: First of all, through the work of this committee and the House, the House passed H.R. 1731, which, in my judgment, is a solid cybersecurity piece of legislation. I hope it or something closely resembling it becomes law. I note that the Senate, with some managers' amendments, offered on the Senate floor the other day, S. 754, which is the Cybersecurity Information Sharing Act. That bill, too, in its current form is, in my judgment, a good piece of legislation. I hope the Senate takes it up on the Senate floor, passes it, and it goes to conference with the House's bill. I want to thank the Members of this committee who were leaders in that effort. We need cybersecurity legislation.

Last thing I will say, and this is probably the most important thing I can say by way of legislation, I cannot deliver for the American public the homeland security that the Congress expects of me and my Department as long as I have to live with the sequestered budget. Unless Congress repeals sequestration, that will have very significant negative effects to our ability to deliver cybersecurity, border security, aviation security, maritime security, work with the FBI and others on other counterterrorism efforts, provide protection for our National leaders, and so forth.

So I urge Congress to repeal sequestration so that we can do what we need to do for the American people. Homeland security is the front line of National security. Thank you.

[The prepared statement of Secretary Johnson follows:]

PREPARED STATEMENT OF JEH C. JOHNSON

OCTOBER 21, 2015

Chairman McCaul, Representative Thompson, and Members of the committee, thank you for the opportunity to be here. I welcome the opportunity to appear before you with Directors Comey and Rasmussen to discuss threats to the homeland and what we are doing to address them. Though I am prepared to discuss the full scope of DHS missions, in these prepared remarks I will focus on: (i) Counterterrorism, (ii) aviation security, and (iii) cybsersecurity.

COUNTERTERRORISM

Last month, I attended a sobering ceremony in Shanksville, Pennsylvania for the 14th anniversary of 9/11. Today, 14 years after 9/11, it is still a dangerous world.

The events on 9/11 were the most prominent and devastating example of terrorist attacks by those who are recruited, trained and directed overseas, and exported to our homeland. The 9/11 hijackers were acting on orders from al-Qaeda's external operations chief, Khalid Sheikh Mohammed, who was in turn carrying out the direction of Osama bin Laden.

Likewise, the attempted "Shoe Bomber" in December 2001, the attempted "Underwear Bomber" in December 2009, the attempted Times Square car bombing in May 2010, and the attempted "Package Bomb" plot in October 2010, were all efforts to export terrorism to the United States, and they all appear to have been directed by a terrorist organization overseas.

The response to these types of attacks and attempted attacks on our homeland was and is to take the fight directly to the terrorist organizations at locations overseas.

But, today the global terrorist threat is more decentralized, more complex, and in many respects harder to detect. The new reality involves the potential for smaller-scale attacks by those who are either home-grown or home-based, not exported, and who are inspired by, not necessarily directed by, a terrorist organization.

Today, it is no longer necessary for terrorist organizations to personally recruit, train, and direct operatives overseas and in secret, and export them to the United States to commit a terrorist attack. Today, with new and skilled use of the internet, terrorist organizations may publicly recruit and inspire individuals to conduct attacks within their own homelands. Al-Qaeda in the Arabian Peninsula no longer

hides the fact that it builds bombs; it publicizes its instruction manual in its magazine, and publicly urges people to use it.

Today, we are also concerned about foreign terrorist fighters who are answering public calls to leave their home countries in Europe and elsewhere to travel to Iraq and Syria and take up the extremists' fight there. Many of these individuals will seek to return to their home countries with that same extremist motive.

On September 29, this committee's bipartisan task force published a report on foreign terrorist fighters. I would like to thank the committee, in particular Chairman McCaul and Ranking Member Thompson, for your work on this important assessment of how we in the U.S. Government can enhance our efforts to counter the threat of foreign terrorist fighters. As noted in the report, the Department of Homeland Security has undertaken much of what is recommended. We have been and are continuing to institute measures to detect and prevent travel by foreign terrorist fighters.

The recent wave of terrorist attacks and attempted attacks here and in Europe reflect the new reality of the global terrorist threat. The Boston Marathon bombing in April 2013, the attack on the war memorial and the parliament building in Ottawa in October 2014, the attack on the Charlie Hebdo headquarters in Paris in January 2015, the attempted attack in Garland City, Texas in May 2015, and the attack that killed five U.S. service members in Chattanooga, Tennessee in July: What does this recent wave of attacks and attempted attacks have in common? They were all conducted by homegrown or home-based actors, and they all appear to have been inspired, but not directed by, al-Qaeda or ISIL.

Finally, we are concerned about domestic terrorism in the form of a "lone wolf" which can include various aspects of domestic terrorism such as right-wing extremism. We devote substantial efforts to study and understand these threats and will continue to further our understanding of the underpinnings of terrorist threats of all forms.

So, what are we doing about it?

The Department of Homeland Security, following the attacks in Ottawa, Canada last October, and in reaction to terrorist groups' public calls for attacks on government installations in the West, directed the Federal Protective Service to enhance its presence and security at various United States Government buildings in Washington, DC and other major cities and locations around the country. We continue this enhanced presence today.

There are presently 38 countries from which we do not require a visa to travel here. This "Visa Waiver Program" is a valuable program to promote trade and travel with our most valued allies. Last November, I directed that, for security reasons, we add fields to the Electronic System for Travel Authorization, or "ESTA" system that travelers from these countries are required to use.

In August 2015, we introduced further security enhancements to the Visa Waiver Program. From now on, countries in the Program will be required to, among other actions, implement arrangements to share information about known and suspected terrorists and serious criminals; collect and analyze travel data; and cooperate with INTERPOL—both for using INTERPOL's Lost and Stolen Passport Database to screen travelers crossing a VWP's country's borders, as well as reporting foreign fighters to multilateral organizations such as INTERPOL or EUROPOL. We also requested permission for the expanded use of U.S. Federal air marshals on international flights from VWP countries to the United States. These security enhancements will enable us to learn more about travelers from visa waiver countries and to more accurately and effectively identify those who pose a security risk before they board planes bound for the United States. These enhancements have already produced tangible security benefits.

Next, given the new reality of the global terrorist threat—which involves the potential for small-scale home-grown attacks by those who could strike with little or no notice—we are enhancing our collaboration with State and local law enforcement. Almost every day, DHS and the FBI share intelligence and pertinent terrorist threat information with Joint Terrorism Task Forces, State fusion centers, local police chiefs and sheriffs. We have also enhanced our information sharing with businesses and critical infrastructure.

With regard to the current refugee crisis, the United States is committed to providing refuge to some of the world's most vulnerable people, while carefully screening refugees for security concerns before admitting them to the United States. The reality is that, with improvements to the process we have made over time, refugees are subject to the highest level of security checks. DHS works in concert with the Department of State, the Department of Defense, the National Counterterrorism Center, and the FBI's Terrorist Screening Center for the screening and vetting of refugees. The U.S. Government conducts both biographic and biometric checks on

refugee applications, including security vetting that takes place at multiple junctures in the application process, and even just before arrival to account for changes in intelligence. All refugees admitted to the United States, including those from Syria, will be subject to this stringent security screening. Acting on my direction, USCIS has developed additional protocols to aid in the identification of security concerns with regard to the Syrian population, and the entire Department, along with the interagency, is committed to continual improvement of overall security vetting, as new techniques or sources of information are identified.

Next, given the nature of the evolving terrorist threat, countering violent extremism in this country is as important as any of our other key missions. Building trusted partnerships with diverse communities is essential to successfully countering violent extremism and curbing threats to the safety of our country. These communities must be empowered to reach those individuals most susceptible to the slick internet appeal of ISIL before they turn to violence. In the last fiscal year, DHS held close to 200 meetings, roundtables, and other events in 14 cities in which I participated. Since becoming Secretary, I have personally met with community leaders in Chicago, Columbus, Minneapolis, Los Angeles, Boston, New York City, Houston, suburban Maryland, and northern Virginia.

We are now taking our CVE efforts to the next level. On September 28, I announced a new DHS Office for Community Partnerships which builds upon the ongoing CVE work across the Department, consolidates our efforts, and takes them to the next level. This office will be the central hub for the Department's efforts to counter the evolving global terrorist threat to our country. I named Mr. George Selim as the director of this Office. George brings significant experience to his new role, having served as the director for community partnerships for the National Security Council since 2012 and previously worked at the DHS Office of Civil Rights and Civil Liberties.

My objectives for this Office are to build upon our partnerships with State and local communities and governments, coordinate and promote relationship-building efforts inside and outside of Government, identify resources to support countering violent extremism through Government-funded grants, public-private partnerships, technology, and philanthropy. Meanwhile, the DHS Office for Civil Rights and Civil Liberties will partner with the Office of Community Partnerships and lead, improve, and expand its important community engagement work, including Community Engagement Roundtables, Town Hall Meetings, and Youth Forums, in cities all across the country.

Finally, our homeland security efforts must also involve public vigilance and action. At the Super Bowl earlier this year, I re-launched the "If You See Something, Say Something"™ public awareness campaign with the National Football League to help ensure the safety and security of employees, players, and fans during Super Bowl XLIX. The newly revamped materials highlight the individual role of everyday citizens to protect their neighbors and the communities they call home by recognizing and reporting suspicious activity. "If You See Something, Say Something"™ is more than a slogan. The public must play an important role in keeping our neighborhoods and communities safe.

AVIATION SECURITY

Since last summer, I have required enhanced screening at select overseas airports with direct flights to the United States. The United Kingdom and other countries have followed suit with similar enhancements, and the European Union passed legislation for both near- and long-term enhancements to cabin baggage screening requirements.

Earlier this year in response to a December incident at the Hartfield-Jackson-Atlanta airport, I asked the Aviation Security Advisory Committee (ASAC) to review and make recommendations to address concerns about whether aviation workers with airport identification badges could bypass security and smuggle weapons or explosives into an operations area or even onto an aircraft. In April, in response to the ASAC's recommendations, I directed the Transportation Security Administration (TSA) to take several immediate actions, including "real-time recurrent" criminal history background checks coordinated with the FBI, reducing the number of access points to secured areas, and encouraging airport workers to report suspicious activity.

I have also prioritized the expansion of preclearance operations at foreign airports with flights to the United States. Preclearance allows U.S. Customs and Border Protection officers overseas to screen passengers bound for the United States at the front end of the flight, protecting the plane, its passengers, and our country, before they even enter the United States. We now have 15 preclearance sites overseas, in

6 different countries, operated by more than 600 CBP Officers and agriculture specialists. The most recent preclearance operation was set up early last year in Abu Dhabi. Since that time, in Abu Dhabi alone, we have already inspected more than 580,000 passengers and crew bound for the United States, and have determined 1,002 individuals to be inadmissible, including a number of them based on National security-related grounds. We are in active negotiations with several countries to expand preclearance operations to ten new foreign airports. I view preclearance as an important piece of our aviation security and our counterterrorism mission.

In May, the Classified, preliminary results of the DHS Inspector General's tests of TSA's screening at airports were leaked to the press. The OIG completed its Classified report last month, and has provided it to the Department and to Congress. The final report recommends corrective measures that TSA is already undertaking. In May and June, I directed a series of actions constituting a 10-point plan to address the concerns raised by the OIG's testing. This plan included a number of immediate and longer-term measures. Under the new leadership of Admiral Peter Neffenger, TSA has promptly begun increasing manual screening and random explosive trace detectors, re-testing and re-evaluating the type of screening equipment tested by the OIG, revising standard operating procedures, and conducting "back to basics" training for every TSA Officer in the country. Many of these measures have either been completed, or soon will be.

CYBERSECURITY

Cybersecurity is critical to homeland security. Cybersecurity is a top priority for me, the President, and this administration.

To be frank, our Federal .gov cybersecurity, in particular, is not where it needs to be. In the case of the breach of the Office of Personnel Management, a large amount of highly personal and sensitive information was taken by a very sophisticated actor. There is a great deal that has been done and is being done now to secure our networks. We do, in fact, block a large number of intrusions and exfiltrations, including those by state actors. But much more must be done.

By law, each head of a Federal department or agency is primarily responsible for his or her agency's own cybersecurity. DHS has overall responsibility for protecting Federal civilian systems from cyber threats, helping agencies better defend themselves, and providing response teams to assist agencies during significant incidents. We have also been able to use the unique authorities given to us by Congress to engage with the critical infrastructure community to reduce the risk that our essential services and functions could be disrupted by a cyber attack.

DHS's National Cybersecurity and Communications Integration Center, or "NCCIC," is the U.S. Government's 24/7 hub for cybersecurity information sharing, incident response, and coordination. Thirteen Federal departments and agencies and 16 private-sector entities have regular, dedicated liaisons at the NCCIC, while over 100 private-sector entities collaborate and share information with the NCCIC on a routine basis.

The NCCIC shares information on cyber threats and incidents, and provides on-site assistance to victims of cyber attacks. In this fiscal year alone, the NCCIC has shared over 15,000 bulletins, alerts, and warnings, responded on-site to 21 incidents and conducted nearly 130 technical security assessments.

It is my personal mission to significantly enhance the Department's role in the cybersecurity of our Government and the Nation. To achieve this, I have directed the accelerated and aggressive deployment of important technologies, guidance, and partnerships that my Department is uniquely situated to provide.

First, we have prioritized full deployment of our EINSTEIN system: An intrusion detection and prevention system that uses Classified information to protect Unclassified networks. I have directed the National Protection and Programs Directorate to make at least some EINSTEIN 3A countermeasures available to all Federal civilian departments and agencies no later than December 31, 2015. We are currently on schedule to achieve this goal. We have also successfully expanded our private-sector version of this program—Enhanced Cybersecurity Services—to all critical infrastructure sectors.

EINSTEIN has demonstrated its value. Since its introduction, E3A has blocked over 650,000 requests to access potentially malicious websites. These attempts are often associated with adversaries who are already on Federal networks attempting to communicate with their "home base" and steal data from agency networks. Importantly, EINSTEIN 3A is also a platform for future technologies and capabilities to do more. This includes technology that will automatically identify suspicious internet traffic for further inspection, even if we did not already know about the particular cybersecurity threat.

Second, DHS helps Federal agencies identify and fix problems in near-real-time using Continuous Diagnostics and Mitigation programs—or "CDM." Once fully deployed, CDM will monitor agency networks internally for vulnerabilities that could be exploited by bad actors that have breached the perimeter. CDM will allow agencies to identify, prioritize, and fix the most significant problems first. It will also provide DHS with situational awareness about Government-wide risk for the broader cybersecurity mission.

Earlier this year, I directed that NPPD make the first phase of CDM available to 97% of Federal civilian departments and agencies by September 30, 2015. We achieved this goal ahead of schedule and are on track to make the second phase available by the end of fiscal year 2016.

Third, information sharing is fundamental to achieving our mission. We must be able to share information in as close to real time as possible while ensuring appropriate privacy protections. We have made excellent progress by leading the development of a system that makes automated information sharing possible. By November, we will have the capability to automate the distribution and receipt of cyber threat indicators. Our partners in the intelligence community and law enforcement have participated in the development of this capability and support the policies that we have put in place to ensure that we have both appropriate privacy protections and the quick dissemination of relevant information to other agencies.

We are working closely with other agencies of our Government to support the stand-up of the ODNI-led Cyber Threat Intelligence Integration Center, or "CTIIC." This is vital because the foreign cyber threats we face as a Nation are too many, too sophisticated, and increasingly too severe to wait any longer to ensure we integrate the intelligence about cyber threats to better inform our defenses and our actions—just as we do with regard to terrorist threats. DHS looks forward to full implementation of this intelligence community initiative, which will help all of the operational cyber centers better understand various strategic cyber threats and provide improved intelligence community support to the NCCIC, which will, in turn, enable us to share more information with our private-sector partners.

Last month, we participated in frank discussions with officials of the People's Republic of China on cyber issues of concern to both our nations. This culminated in our President's announcing several key cybersecurity commitments. As part of these commitments, we agreed to investigate cyber crimes, collect electronic evidence, and mitigate malicious cyber activity emanating from its territory, and to provide timely responses to requests for information and assistance concerning those activities. Both sides also agreed to provide updates on the status and results of those investigations and to take appropriate action. As part of this commitment, we agreed to establish a high-level joint dialogue mechanism on fighting cyber crime and related issues. Perhaps most importantly, the United States and China committed that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. The United States and China also committed to create a senior experts group on international security issues in cyber space.

Time will tell whether the Chinese will live up to these commitments. I intend to remain personally engaged on these issues, to ensure that China takes concrete steps to advance progress made thus far. To be sure, these commitments do not resolve all our challenges with China on cyber issues. But, they do represent a step forward in our efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship. On the U.S. side, we are prepared to fulfill our commitments. Words must be matched by actions.

We cannot detect and stop every cyber single intrusion. So often, the most sophisticated actors penetrate the gate through a simple act of spearphishing, because they know they can count on a single user letting his guard down. But, we have made considerable progress and continue to take aggressive action.

I urge Congress to act by passing cyber legislation. I applaud the bipartisan work that has been done so far in this Congress. We need legislation to accomplish at least two things:

First, we need explicit Congressional authorization of the EINSTEIN program. This would eliminate any remaining legal obstacles to its deployment across the Federal Government. The House has passed H.R. 1731, which accomplishes this and ensures agencies understand they are legally permitted to disclose network traffic to DHS for narrowly-tailored purposes.

Second, we need the Senate to finish its work on the Cybersecurity Information Sharing Act as soon as possible. This committee's engagement with the bill's sponsors has strengthened the legislation and incorporated important modifications to better protect privacy. I understand that work continues to make necessary changes,

and we greatly appreciate those efforts. But cyber criminals are not waiting to steal intellectual property or financial data, so neither can Congress wait to pass information-sharing legislation. I urge you to call upon Senate leadership to bring this bill up as soon as possible so that the Senate can finish its work and pass it.

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. Thank you, and I look forward to your questions.

Chairman MCCAUL. Thank you, Secretary. I certainly agree, and we need to reprioritize our budget towards National security and National defense. On the cybersecurity bill, I am glad we are able to enhance, I think, the Senate version more towards the House effort, and I think we will have a successful conference committee. That is why I have great hope and deliver for you, so you can do a better job at that important effort. Finally, thank you for your recognition of the report itself in the task force.

With that, the Chair now recognizes Mr. Rasmussen.

STATEMENT OF HON. 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 the committee Members. Like Secretary Johnson and Director Comey, I welcome today's opportunity to discuss a range of threats to the homeland that concerns us the most. But before getting into that threat picture in some detail, I want to stress that we at NCTC are very closely aligned with DHS, with FBI, and our other counterterrorism community and intelligence community partners in terms of how we view that threat environment.

From an analytic perspective, I would start by saying, that the chances of a spectacular, large-scale attack in the homeland by an overseas terrorist group have been substantially reduced over the last several years. We have collectively achieved that outcome through aggressive CT action against al-Qaeda overseas and through the robust homeland security infrastructure that we have developed as a country in the last 14 years.

But while we can look with some degree of satisfaction that the work done to reduce that threat of a large-scale mass casualty attack, there is still quite a bit to be concerned about on the current terrorism landscape. That landscape, as you yourself said, Mr. Chairman, is, in some ways, more challenging than ever. It is also clear that the terrorist-operating paradigm has shifted, and it has shifted in ways that are proving particularly challenging as we try to identify and disrupt potential threats to the homeland.

Today, there are more threats originating in more places and involving a more diffuse and disparate set of individuals than at any time previously.

Now, first, as you would expect, we are intensively focused on the threat of ISIL, which you highlighted in your opening statement, Mr. Chairman. In our judgment, ISIL has overtaken al-Qaeda as the leader of the global violent extremist movement, and the group views itself as being in direct conflict with the West. That conflict

is increasingly being played out not just in Iraq and Syria, but also in other places around the world where ISIL has declared itself to have a province. These places include Algeria, Libya, Egypt, Yemen, Saudi Arabia, Afghanistan and Pakistan, Nigeria, the Caucasus region, potentially in Southeast Asia as well. ISIL's aggressive growth and expansionist agenda has implications for us here at home, in our homeland threat picture, and there are three especially concerning features of ISIL as a terrorist group, in my judgment. The first is their access to resources, extensive resources, in terms of manpower, military materiel, and funds.

The second concerning feature of ISIL is the territorial control the group exercises in Iraq and Syria as well as in some of the provinces I mentioned a minute ago. The third, again, is something that you highlighted in your remarks, Mr. Chairman, their access to a large pool of individuals from Western countries, both those who have traveled to Iraq and Syria, and those who have remained in their home countries.

When we look for indicators of potential external operations capability that could threaten the homeland from ISIL, these are the key features we generally expect to see, and they are present with ISIL. Secretary Johnson also alluded to how we are coming to view the threat from ISIL, especially the homeland piece of that threat. We started to view ISIL's involvement in homeland attack activity as falling along a spectrum. At one end of that spectrum, we see isolated individuals who draw inspiration from ISIL's highly sophisticated media content, even if ISIL leadership is not directly guiding their actions.

At the other end of the spectrum, something more traditional, we assess that there are individuals who may, in fact, receive direct guidance and specific direction from ISIL members. More often than not, individuals we see here in the homeland tend to operate somewhere between those two ends of the spectrum, creating a fluid picture that is difficult to assess.

Second, if you look beyond our intensive focus on ISIL and the threat it poses to the homeland, we continue to devote substantial attention to al-Qaeda and its affiliates and nodes around the world. Despite the unrelenting media attention focused in ISIL, in no respect would I or our intelligence community downgrade our intention on al-Qaeda-related threat activity in favor of greater focus on ISIL. In fact, when I am often asked in public settings to identify what my No. 1 terrorism concern is, I decline to answer, because I would not want our focus on one terrorist threat to suggest that we are not focused on other significant threats that we are confronting.

Specifically, right now we are closely watching for signs that core al-Qaeda's attack capability is potentially being restored ahead of the U.S. military's drawdown in Afghanistan. While the ability of al-Qaeda to train, recruit, and deploy operatives from their safe haven in South Asia has been degraded, we continue to watch for and track indications that core al-Qaeda is, in fact, engaged in plotting activity aimed at the homeland.

In the statements for the record, both Director Comey and Secretary Johnson singled out al-Qaeda in the Arabian Peninsula for particular attention, and that is for good reason. The threat from

AQAP remains at the top of our list of analytic priorities, given the group's unrelenting focus on targeting U.S. interests, including potentially the aviation sector.

Beyond Yemen, we have also been watching al-Qaeda's affiliated networks of individuals in Syria who may be looking to carry out external operations against the West, or potentially the homeland. While we have had some very public successes in terms of disrupting some of the individuals involved in that plotting from Syria, there is clearly more to be done in this regard, and the work continues.

Our third area of priority, my last area that I will mention in my remarks, is the growing use of simple opportunity-driven attacks by home-grown violent extremists, what we call HVEs. That style of attack has clearly proliferated within the last several years. When you look back to 2009, we were seeing, on average, less than 2 or 3 of those incidents per year. By last year, 2014, that number was a dozen, and to date, this year, that number of incidents, or disruptive plots, have already doubled for this year, suggesting that there are, in fact, a greater number of HVEs inside the United States pursuing potential attack plans.

While it is very difficult to put precise numbers on that population of home-grown violent extremists here in the United States, there is no question in my mind and in the mind of our analysts that this population has increased in size over the last 18 months.

In my judgment, ISIL has injected new energy and life into that population of home-grown violent extremists. ISIL, for its part, knows that it can have a real impact by motivating individuals to act in their own locations by carrying out individual attacks, even on a relatively modest scale. That is particularly true of several such attacks when strung together in a compressed time frame. That is a significant innovation in the terrorist playbook, something that al-Qaeda never quite managed to deploy against us, and it requires that we in the counterterrorism community innovate and adapt as well.

To conclude, Chairman and Congressman Thompson, I want to assure you and the rest of the committee that we continue to work every day to detect, defeat, and disrupt all manner of threats from across this full spectrum of terrorist concerns that we have. I look forward to discussing these issues with you and the committee in greater depth.

[The prepared statement of Mr. Rasmussen follows:]

PREPARED STATEMENT OF NICHOLAS J. RASMUSSEN

OCTOBER 21, 2015

Thank you Chairman McCaul, Ranking Member Thompson, and Members of the committee. I appreciate this opportunity to discuss the threats that concern us most. I'm pleased to join my colleagues and close partners from the Department of Homeland Security and Federal Bureau of Investigation.

THREAT OVERVIEW

With the fourteenth anniversary of the 9/11 attacks several weeks behind us, it's clear that we've had great success at substantially reducing the chances of that kind of attack recurring. We've done that not only with aggressive CT action against core al-Qaeda in South Asia and around the world but also through the array of defenses we've erected as a country. The counterterrorism and homeland security infrastruc-

ture that exists gives us much greater defense, disruption, and mitigation capabilities that we did not have at the time of those attacks.

That said, the array of extremist terrorist actors around the globe is broader, wider, and deeper than it has been at any time since 9/11, and the threat landscape is less predictable. While the scale of the capabilities of these violent extremist actors does not rise to the level that core al-Qaeda had at its disposal at the time of 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 last 14 years.

We remain intensely focused on the threat from ISIL. There is no doubt that the group views itself as being in direct connect with the West. 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 at as being critical to the development of an external operations capability. We are very concerned and focused on ISIL's trajectory in this regard. ISIL must also win the war on the ground in Syria and Iraq, which remains, we believe, a top priority for the group's leadership. This is in addition to advancing their effort to establish and administer branches in areas further afield, branches that are demonstrating increased operational capabilities in their respective regions.

We are coming to view the threat from ISIL as a spectrum, where on one end, individuals draw inspiration from ISIL's media content and perceive successes. At the other end, individuals may receive direct guidance from ISIL members. These ends of the spectrum are not polar opposites, however. Rather, they are the clearest illustrations of what is more often than not a very fluid picture where individuals operate between the two extremes.

The tremendous efforts being made 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 being a principal counterterrorism priority. We would not tier our priorities in such a way that downgrades al-Qaeda in favor of greater focus on ISIL. When we are looking at the set of threats that we face as a Nation, al-Qaeda threats still figure prominently in that analysis.

The steady attrition of al-Qaeda senior leaders has put more and more pressure on the few that remain. We believe we have constrained both their 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 resident in the tribal areas of Pakistan or in eastern Afghanistan has been eliminated entirely.

Ahead of the U.S. military's draw-down in Afghanistan, we in the intelligence realm are trying to understand the level of risk the United States may face over time if al-Qaeda regenerates, finds renewed safe haven, or restores lost capability. I am confident that we will retain sufficient capability to continue to put pressure on that core al-Qaeda network so that that situation will not arise.

We as an intelligence community will be very much on alert for signs that that capability is being restored, and we would warn immediately should we find ourselves trending in that direction. All that said, I'm still not ready to declare core al-Qaeda as having been defeated in the classical sense of the word where the capability has been removed. So long as the group can regenerate capability, al-Qaeda will remain a threat.

We also see increasing competition between 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 that we will watch 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. The difficulty in collecting precise intelligence on terrorist intentions and the status of particular terrorist plots is increasing over time.

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 group's innovative and agile use of new means of communicating, including ways in which they understand are beyond our ability to collect. I know that FBI Director Carney has spoken about these challenges on a number of occasions.

Second, while we've seen a decrease in the frequency of large-scale, complex plotting efforts that sometimes span several years, we've seen a proliferation of more rapidly-evolving threat or plot vectors that emerge simply by an individual encouraged to take action, then quickly gathering the few resources needed and moving

into an operational phase. This is something I would tie very much to the modus operandi of ISIL-inspired terrorists. The so-called "flash-to-bang" ratio 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. In terms of propaganda and recruitment, they can generate further support for their movement, 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 growing 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 diminish the appeal of terrorism and dissuade individuals from joining them in the first place.

To this end, we continue 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 the tools they need to see extremism in their midst and do something about it before it manifests itself in violence. NCTC, in direct collaboration with DHS, has led the creation of CVE tools to build community resilience across the country.

Working and closely coordinating with the Department of Justice (DOJ), the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI), NCTC is engaged in this work all across the country.

We, in concert with DOJ, DHS, and FBI, 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, developed in partnership with DHS, 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.

This is not a law enforcement-oriented effort designed to collect information. Rather, it is an effort to share information about how members of our communities are being targeted and recruited to join terrorists overseas. Seen in that light, we have had a remarkably positive reaction from the communities with whom we have engaged.

We continue to expand our CVE tools. With our DHS colleagues, we have created and regularly deliver 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.

We also aim 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

In summary, confronting these threats and working with resolve to prevent another terrorist attack remains the counterterrorism community's overriding mission. I can assure you that we at NCTC are focused on positioning ourselves to be better prepared to address the terrorist threat in the coming years. We expect this threat will increasingly involve terrorists' use of the on-line platforms that I mentioned earlier in my remarks.

Chairman McCaul, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to testify before you this morning. I want to assure you that our attention is concentrated on the security crises in Iraq and Syria—and rightly so—but we continue to detect, disrupt, and defeat threats from across the threat spectrum in concert with our partners.

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

Chairman MCCAUL. Thank you, sir. We appreciate the work that you do.

The Chair now recognizes Mr. Comey.

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

Mr. COMEY. Thank you, Mr. Chairman, Mr. Thompson, Members of the committee. Thank you for inviting me here today. My colleagues have made clear in their opening statements something that I won't repeat, that ISIL has broken the model.

I want to explain why that change in model leads us to talk so much about the challenges we face with encryption very briefly. Social media has transformed human experience in wonderful ways. I have no idea where anybody from my fifth grade class at P.S. 16 in Yonkers, New York is today. My kids will know everything about everybody from their fifth grade class for the rest of their life. There is good and bad to that. I think, on balance, it is wonderful. But ISIL has used that ubiquitous social media to break the model and push into the United States, into the pocket, onto the mobile devices of troubled souls throughout our country in all 50 States a twin message, come or kill, come or kill. Come to the so-called caliphate, live a life of glory, participate in the final battle between good and evil on God's side. Come to the caliphate, and if you can't come, kill where you are.

Social media works to connect us. It works as a way to sell cars or shoes or a movie. It works to crowdsource terrorism. So starting in the summer of 2014, they really invested in this, and it works. It led to troubled souls convincing themselves that there was meaning for them in Syria and Iraq, or that they should engage in acts of violence in the United States, and that investment started to pay dividends, and taxed all of our resources in the spring of this year, when suddenly we had dozens and dozens of cases in the United States of people who were progressing along the spectrum from consuming to acting to killing where they are. Thank goodness, thanks to tremendous work by the men and women who work for us, that was disrupted. We arrested dozens of people during this year to disrupt those plots.

The challenge we face is enormous, because this broken model, this crowdsourcing of terrorism means there are hundreds of people across our great country who are troubled, who are consuming this poison. We have investigations in all 50 States trying to understand. So where are they from consuming to acting? Very hard to find them and to evaluate them. It gets harder still. It is not just a Nation-wide haystack where we are looking for needles, ISIL makes those needles disappear on us. Because if they find a live one through Twitter, they will move them through all these investigations to an end-to-end mobile messaging app that is encrypted, and then the needle disappears. So we know if somebody is really dangerous to us, the needle goes invisible to us. That is very, very concerning.

The reason we are talking so much about encryption is we see in ISIL, and more broadly, a conflict between two values everybody in America cares about. We all care about safety and security on the internet. I and Nick and Jeh are huge fans of encryption, right?

We want our key data encrypted. It helps the FBI fight cyber intrusions. That value, safety and security, is colliding with public safety, which we all care deeply about. We don't have an easy answer, but a great democracy should see when its values are in collision and talk about how we might resolve those two things.

There is no easy answer. The good news is we are having productive conversations with local law enforcement, which cares deeply about this, with our allies, and with the companies who make these devices and offer these services, because they are good folks who care about both values. This is a really hard problem for our country. We are not here to tell what the answer is. We are here just to tell folks. The example I use is, the FBI is not an alien force imposed on America from Mars, right? We belong to the American people. We have the tools the American people gave us through you; and our job, when one of those tools isn't working so much anymore, is to tell the American people. That is why we are talking so much about encryption. You see it in the ISIL cases, you see it in kidnapping cases, drug cases, child abuse cases. There is a conflict in our values that we simply must figure out how to resolve. It is obvious in the case of ISIL. We will continue doing the work.

I am very grateful, as my colleagues are, for the high-quality product that this committee did on travelers, those responding to the first part of that siren song, that "come." There is something interesting happening that I want to tell the committee about. Just in the last few months, we are seeing fewer people attempt to travel to join ISIL in Syria. We have seen 6 in the last 3½ months. We were seeing 9 a month in all the months before that.

I don't know what to make of that. One possibility is we are not seeing it the way we were before; they are still going. Another possibility is all of our efforts to lock people up and punish them for going is making a difference, another difference is help from our colleagues around the world, especially the Turks, or something else. But we are starting to notice that curve, which was going up like a hockey stick, flatten a little bit. We will keep you posted on whether that continues, but this committee has done such great work on that topic, I wanted you to know that fact. We are very grateful for the opportunity for this conversation.

[The prepared statement of Mr. Comey follows:]

PREPARED STATEMENT OF JAMES B. COMEY

OCTOBER 21, 2015

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 communicate—both to inspire and recruit. The wide-spread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the homeland or abroad. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. Our successes depend on interagency cooperation. We work closely with our partners within the Department of Homeland Security and the National Counterterrorism Center to address current and emerging threats.

COUNTERTERRORISM

Counterterrorism remains the FBI's top priority, however, the threat has changed in two significant ways. First, the core al-Qaeda tumor has been reduced, but the

cancer has metastasized. The progeny of al-Qaeda—including AQAP, al-Qaeda in the Islamic Maghreb, and the Islamic State of Iraq and the Levant (ISIL) have become our focus.

Secondly, we are confronting the explosion of terrorist propaganda and training on the internet. It is no longer necessary to get a terrorist operative into the United States to recruit. Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they can't travel, they motivate them to act at home. This is a significant change from a decade ago.

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

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

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al-Qaeda or other foreign terrorist organizations, ISIL has persistently used the internet to communicate. From a homeland perspective, it is ISIL's wide-spread reach through the internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life—from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is 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.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred when an individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

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

ISIL continues to disseminate their terrorist message to all social media users—regardless of age. Following other groups, ISIL has advocated for lone-offender attacks. In recent months ISIL released a video, via social media, reiterating the group's encouragement of lone-offender attacks in Western countries, specifically advocating for attacks against soldiers and law enforcement, intelligence community members, and Government personnel. Several incidents have occurred in the United States and Europe over the last few months that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

In one case, a New York-based male was arrested in September after he systematically attempted to travel to the Middle East to join ISIL. The individual, who was inspired by ISIL propaganda, expressed his support for ISIL on-line and took steps to carry out acts encouraged in the ISIL call to arms.

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

Social media has allowed groups, such as ISIL, to use the internet to spot and assess potential recruits. With the wide-spread horizontal distribution of social

media, terrorists can identify vulnerable individuals of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

In other examples of arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly-accessed social networking sites, but others take place via private messaging platforms. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland.

We live in a technologically-driven society and just as private industry has adapted to modern forms of communication so too have terrorists. Unfortunately, changing forms of internet communication and the use of encryption are posing real challenges to the FBI's ability to fulfill its public safety and National security missions. This real and growing gap, to which the FBI refers as "Going Dark," is an area of continuing focus for the FBI; we believe it must be addressed given the resulting risks are grave in both traditional criminal matters as well as in National security matters. The United States Government is actively engaged with private companies to ensure they understand the public safety and National security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time.

The FBI is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the on-going threat posed by foreign terrorist organizations and home-grown violent extremists. We continue to encourage robust information sharing; in partnership with our many Federal, State, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information-sharing processes as well as pursue technological and other methods to help stay ahead of threats to the homeland.

INTELLIGENCE

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken two steps to improve this integration. First, we have established an intelligence branch within the FBI headed by an Executive Assistant Director ("EAD"). The EAD looks across the entire enterprise and drives integration. Second, we now have Special Agents and new Intelligence Analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better-prepared to work well together in the field. Our goal every day is to get better at using, collecting, and sharing intelligence to better understand and defeat our adversaries.

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

CYBER

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

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

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques—such as sources, court-authorized electronic surveillance, physical surveillance, and forensics—to fight cyber threats. We are working side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF), which serves as a coordination, integration, and information-sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations. Through CyWatch, our 24-hour cyber command center, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to Federal cyber centers, Government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We 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 and terrorists' use of the internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the homeland, and the impact of the Going Dark problem on mitigating their efforts. I am happy to answer any questions you might have.

Chairman MCCAUL. I thank you, Director.

The Chair now recognizes himself for questioning.

Let me say, on the encryption issue, Dark Space platform, this committee is—we are meeting with technology companies trying to find a solution to that. You have the foreign fighter threat, but the threat over the internet is real; it has gone viral. I think the good news is Junaid Hussain was taken out by an air strike. That is publicly reported, and had some impact, I think, but it is going to continue until we find a solution, a technology solution.

I also want to commend you for the success both you and the Secretary have had in stopping so many plots. We put out a monthly terrorist snapshot, and the fact is, every month these numbers go up in terms of terror plots. We had 17 terror plots here in the United States, ISIS-directed or inspired, and overall, almost 70 ISIS-related individuals arrested. You don't know what you don't know. The Chattanooga case is a good example. You can't stop all this. The chatter is so high, it is hard to stop all of it.

My first question, just very simply, is—and I will direct it to the Secretary—is: Do you consider the threat environment to the homeland to be one of the greatest since 9/11?

Secretary JOHNSON. Chairman, like Nick, I tend not to rank threats or rank periods——

Chairman MCCAUL. Use your mike.

Secretary JOHNSON. I tend not to rank threats or try to make an assessment that a current period is more or less dangerous than

before, because we have to focus on a number of things. The point that I want to stress is that it is different. It is different than what it was in the 9/11 period in that it is more decentralized and more diffused; it is more complicated because of the going—Going Dark phenomenon because of the very effective use of social media, and because of the potential for the lone actor, who isn't necessarily exported from overseas, but who could strike here at any moment, which requires a more complex response, a more whole-of-Government response.

We are very concerned. I am encouraged by the numbers Jim cited of those we know about who have attempted to leave, but we also know that ISIL is still out there every day making an appeal. So we have got to stay busy.

Chairman MCCAUL. Director Comey.

Mr. COMEY. I think about it the way Jeh does. In some ways, we are demonstrably safer, thanks to the work of this committee and the whole of Government. This—our country is better organized, better deployed, smarter, tougher than we were before 9/11. So as Director Rasmussen said, I agree that the threat of the big thing is not gone, but it is diminished significantly. At the same time, there has been a metastasis of the threat in all of the likely governed or ungoverned spaces throughout the world.

We are obviously all looking at Libya closely now, and the Sinai, and lots of other parts of the world. So it has been more diffuse. It moves at us faster through social media, and there is a whole lot more people in the United States—energized, troubled souls—than there were by core al-Qaeda at or after 9/11. So it is just very different today.

Chairman MCCAUL. Mr. Rasmussen.

Mr. RASMUSSEN. The only thing I would add to that is that the diffusion and the dispersal of the threat that all three of us have talked about creates a particular problem in that it stretches our resources that much more widely. The blanket has to cover more of the bed. When you look around the world, all of the locations, all of the safe haven locations, all of the regions of instability around the world where a potential terrorist threat might emanate from are areas where we have to look to enhance our collection of intelligence, enhance our ability to partner with governments in those regions, and that is just a resource challenge.

If you think about the period dealing with core al-Qaeda, we were focused pretty extensively on Pakistan and Afghanistan, now you could rattle off 12 or 15 countries where we are very, very active.

Chairman MCCAUL. That is more of a global limit.

Let me move quickly to the latest edition of *Dabiq,* which is ISIS's basically *Inspire* magazine. They discuss the idea of moving a weapon of mass destruction through transnational criminal organizations into the Western Hemisphere and across the Southwest Border from Mexico into the United States. Being from Texas, this certainly concerns me, and, of course, not getting into specifics, but a plot was disrupted out of Moldova, trying to smuggle to Islamist terror organizations, nuclear materials that could have reached our shores. Director Comey, how serious do you take this threat?

Mr. COMEY. Deadly seriously. This is something that we have worried about for a long time. We have a division of the FBI, the Weapons of Mass Destruction Directorate, where people wake up every single day worrying about this. It is one of the reasons that we have tried to build such good relationships with our law enforcement colleagues in so many of the places where there might be materials available, including the former Soviet States. So it is the classic, extremely low-probability, extraordinarily high-impact event, so it has our constant focus.

Chairman MCCAUL. My final question is on the Syrian refugees. We have had testimony before this committee that we don't have intelligence on the ground in Syria. We can't properly vet these individuals through databases. We don't know who they are. I visited a camp in Jordan with some Members on the committee, and we were told the same thing. I know the administration is planning on moving as high as 10,000 refugees into the country. Just very quickly, as my time is running out, how concerned are you from a security perspective on this? Do you think this will increase your counterterrorism caseload if we bring in 10,000 Syrians into the United States? Secretary Johnson.

Secretary JOHNSON. Chairman, we—I am concerned that we do the proper security vetting for refugees we bring into this country. We committed to 10,000, and I have committed that each one will receive a careful security vetting. It is true that we are not going to know a whole lot about a lot of the Syrians that come forth in this process, just given the nature of the situation. So we are doing better at checking all the right databases and the law enforcement and intelligence communities than we used to, and so it is a good process, and it is a thorough process, but that definitely is a challenge.

Chairman MCCAUL. Director Comey.

Mr. COMEY. I don't think I have anything to add to Jeh. I think he describes it well. We see a risk there. We work hard to mitigate it. Our challenge will be, as good as we have gotten ourselves at querying our holdings to understand somebody, if the person has never crossed our radar screen, there won't be anything to query against, and so we do see a risk there.

Chairman MCCAUL. Well, for the record, we are a humanitarian Nation. It is a humanitarian crisis, but we also have a responsibility to protect the American people, and to me, that is paramount as well.

The Chair now recognizes the Ranking Member.

Mr. THOMPSON. Thank you, Mr. Chairman. Taking off from your question relative to the Syrian refugees, can each of you explain your agency's position on the vetting process for these refugees? A lot of us are concerned about whether or not you have enough information available to you to do an accurate vetting. So, Mr. Rasmussen, can you——

Mr. RASMUSSEN. Sure. I am happy to start.

As Director Comey suggested, we have a lot of lessons learned in this area from when we went through similar processes over the last several years dealing with other large refugee populations. So, I think we have now worked successfully to make sure that every bit of available intelligence information that the United States

Government holds will be looked at with respect to a potential nexus to someone being screened as a potential refugee.

I certainly feel good about that process and the degree to which we have tightened that up over time. You can't account for what you don't know, and that goes to the intelligence deficit that I think is embedded in your question. What we can do, though, is understand where the potential vulnerabilities are so that we are asking in the screening and vetting process the right kinds of questions to give our screeners and vetters the best possible opportunity to make an informed judgment. It is not a perfect process; there is a degree of risk attached to any screening and vetting process. We look to manage that risk as best we can.

Mr. THOMPSON. Mr. Secretary.

Secretary JOHNSON. Each of us at the table here is acutely aware that in our world, one failure is the equivalent of 10,000 successes. There are, in fact, lessons we learned from the vetting process with regard to the Iraqi refugees that we took in. The process has improved. We are better at connecting dots, checking the databases with information we have.

My people in USCIS, to do this, will be on the ground in places to vet refugees along with the State Department, but they will do so in consultation with our law enforcement and our intelligence agency partners. We will do it carefully. We have made this commitment, but we will commit the resources to do it, and we will do it carefully.

Mr. THOMPSON. Mr. Director.

Mr. COMEY. I don't think I have anything useful to add. I think my view was captured by what both the Secretary and the Director said.

Mr. THOMPSON. So I—capsuling what has been said, it is your feeling that our existing systems are robust enough to assure this committee that, to the extent practical, no terrorist can get through that process?

Secretary JOHNSON. Well, the issue we face, obviously, is what Jim mentioned. We may have somebody who comes to us and is simply not on our radar for any discernable reason. It may also be the possibility that somebody decides to do something bad after they have been admitted through the process. But we do have a good system in place for the undertaking that we have made.

Mr. THOMPSON. Mr. Director, before this committee, Assistant Director Steinbach said that the concerns in Syria is that we don't have the systems in place on the ground to collect the information to vet. That would be the concern: Databases don't hold the information on these individuals. Is that still the position of the Department?

Mr. COMEY. Yes. I think that is the challenge we are all talking about, is that we can only query against that which we have collected. So, if someone has never made a ripple in the pond in Syria in a way that would get their identity or their interests reflected in our database, we can query our database until the cows come home, but we are not going to—there will be nothing to show up, because we have no record on that person.

That is what Assistant Director Steinbach was talking about. You can only query what you have collected. With respect to Iraqi

refugees, we had far more on our databases because of our country's work there for a decade. This is a different situation.

Chairman MCCAUL. The Chair recognizes Mr. Smith from Texas.

Mr. SMITH. Thank you, Mr. Chairman. I just want to get some figures on the table. I understand the administration wants to admit about 15,000 Syrian refugees this year and as many as 25- to 30,000 next year. Is that generally correct?

Secretary JOHNSON. The number this year is 10,000.

Mr. SMITH. Ten thousand. Then next year would be how many?

Secretary JOHNSON. I don't believe that a firm decision has been made with respect to fiscal year 2017, but this year, we said we want to take in 10,000.

Mr. SMITH. It has been reported that there would be 2 to 3 times that many next year, much more of a significant increase.

You have all used the word "risk" to describe admitting these refugees, and I assume that what we have heard and read is accurate, and that is that terrorist organizations are going to be tempted to try to infiltrate these refugees and try to sneak individuals into this country who might commit terrorist acts. I guess the question I have for you is, how likely is it that terrorist organizations are going to try to take advantage of the admission of these refugees to get people in this country who might commit terrorist acts? Is it likely? Not likely?

Secretary JOHNSON. That is an intelligence question.

Mr. RASMUSSEN. We have certainly seen terrorist groups talk about, think about exactly what you are describing, Mr. Smith, trying to use available programs to get people not only in the United States, but into Western European countries as well. So we know that they aspire to do that. I don't know that I would go so far as to say they are likely to succeed, because, again, we——

Mr. SMITH. Is it possible to conduct background checks on these individuals, or is it only if they are already in the database that they would be flagged? In other words, the terrorist organization isn't going to try to get someone in as a refugee if they already have a public background that you would be able to uncover. They are going to get people into the country who have not yet committed a terrorist act. Don't you think it is likely that they are going to try to do that?

Secretary JOHNSON. There is a pretty thorough vetting process of each individual, which encompasses a personal assessment of each individual, which includes an interview. It is not just simply what is in a public record, does the person have a rap sheet of any kind. So there is that personal assessment.

Mr. SMITH. That is a little bit of my concern. You are relying upon them and what they say or what they write out in an application, and you can't go beyond that. So you are sort of having to take their word for it.

Another red flag to me is that I—in past years, historically, traditionally, refugees have been members of families, and yet, the typical profile of a Syrian refugee, I am told, is that most are young, single males as opposed to family members. So to me, that would raise a red flag as well. Do you have any information, any comments, about that?

Secretary JOHNSON. Coming from me, sir, the one observation I have of resettled Syrian refugees in this country so far is that they tend to settle into communities that are very—that embrace them, that are very supportive in Syrian American communities around the country. I have seen that personally myself. It tends to be a pretty tight-knit and supportive community.

Mr. SMITH. Okay. Well, as I say, both the profile and the motives of terrorist organizations and your admission that there is some risk involved, to me, would persuade the administration to go slow rather than fast when it comes to admitting individuals who might not—who might do us harm.

Secretary Johnson, let me move to another subject. The administration—this is more of a domestic concern. The administration has announced that next month, it is going to release a number of thousands of individuals from Federal prison. How many individuals is the projection that will be released next month? These are criminal aliens.

Secretary JOHNSON. Well, the total number that the Department of Justice plans to release pursuant to their guidelines adjustment next month, I am told, is about 2,000.

Mr. SMITH. Two thousand.

Secretary JOHNSON. Yes.

Mr. SMITH. Then how many of those individuals will be put into the process to be removed?

Secretary JOHNSON. A fair number. This is something—let me—let me stress, this is something that we have been working on now for about a year, and the thing that I am focused on, that I have been focused on, those who are released who are undocumented, that they come directly into our custody, that they are not released into the streets.

Mr. SMITH. Good. Good.

Secretary JOHNSON. So I believe that process, because I have checked numerous times, is in place, and that is exactly what is going to occur.

Mr. SMITH. Good. Last time you appeared before this committee, I brought up the figure that the administration is releasing close to 30,000 people every year who have been in prison, been arrested, mostly convicted, and released them back out into our communities and neighborhoods. You said that figure was going to go down dramatically; it needed to stop. I have heard that for a couple of years now. Is the administration still releasing individuals back into our communities who are in the country illegally, who have been convicted of crimes, or are those individuals being put into removal procedures now?

Secretary JOHNSON. Well, Mr. Smith, as I am sure you are aware, if someone is in immigration detention with a final order of removal, the law says that we have to do a 6-month assessment.

Mr. SMITH. Right.

Secretary JOHNSON. If repatriation is not imminent, there are only limited circumstances under which we can hold them. I have changed the process for deciding the circumstances under which that happens. We don't have the final numbers yet for fiscal year 2015, but I believe that the number of those who have been re-

leased who have been convicted of crimes has gone down from 30,000.

Mr. SMITH. To what number?

Secretary JOHNSON. I don't have the number yet. But I am told it has gone down from 30,000. Fiscal year 2013 was about 34, as I am sure you will recall; 2014 was about 30; and I believe the number is south of 30 for fiscal year 2015.

Mr. SMITH. I hope it is very far south of 30 for the sake of innocent American citizens. Thank you.

Chairman MCCAUL. Thank you.

I just want to state for the record that ISIS has been on record through a smuggler stating that they want to exploit the refugee process to infiltrate the West. I take them at their word. So I would caution the administration to proceed very carefully in this program.

The Chair recognizes Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank you, and I want to thank our witnesses for being here today, and your testimony.

I am going to turn to another trifecta, and that is going back to the issue of cybersecurity, which we have referenced a couple of times here today. I thank the Chairman for his leadership on this issue and the Ranking Member.

Mr. Secretary, you reference, and you have spoken about this before, the recent breach of OPM's networks and the role DHS has in protecting agency networks, and I understand that the leadership at OPM at the time was asleep at the switch and that they certainly ignored warnings from their own inspector general. I know that DHS to provide tools, EINSTEIN CDM, to assist agencies. So I have to ask you at this point for an update. You know, I—can you tell me with confidence that other agencies under your care will not suffer breaches like OPM's?

Secretary JOHNSON. I can tell you that we are making rapid and significant progress to ensure that does not happen. The EINSTEIN 3A system right now, which has the ability to block intrusions, is available and deployed to about half the Federal civilian government.

I have directed my folks at DHS to make it available to 100 percent by the end of this year, and I believe we are on track to do that.

We have gotten agency heads who, by law, are responsible for their own cybersecurity to focus on this issue. I issued a binding operational directive in May pursuant to authority given to me by the Congress to do that, which is, in effect, a scorecard to get agency heads to focus on this issue, and we have a very aggressive plan for enhancing our diagnostics ability.

So I believe that awareness in these agencies has been enhanced significantly, including because of the OPM breach, and that we are on an aggressive time table to cross the Federal Government to ensure that this kind of thing can't happen, or that the risk of it happening is significantly reduced.

Mr. LANGEVIN. So on the issue of binding operational directives, I want to know, and this is basically authority pursuant to what Congress says, has authorized, but how does it work and what are

the consequences if a binding operational directive is ignored by the agency?

Secretary JOHNSON. Well, basically, the way the authority works that Congress has given me, I have the ability to go to each agency and say, here is—here are your vulnerabilities; you need to clean them up by a certain date. If you don't, they will be highlighted, and we will have to follow up with you on this.

Mr. LANGEVIN. They will be highlighted, but what does that mean? What is the consequence if they ignore your binding operation——

Secretary JOHNSON. My recollection—my recollection—now I am working on recollection—is that it means a report to Congress and a report to OMB. But I don't have the authority to simply do that job for an agency head myself, or in any way fine them or sanction them.

Mr. LANGEVIN. That is a frustration which, you know, I have been talking about for a long time. I think you or somebody needs that authority.

Mr. Secretary, before my time runs out, do you still believe that agencies should have primary responsibility for their network defense?

Secretary JOHNSON. I believe that agency directors, administrators themselves should be principally responsible for their own networks. I also believe that DHS should have the overall responsibility for the security of the Federal Civilian.Gov system, but it should be on each agency head to take responsibility for his or her own networks.

Mr. LANGEVIN. Right. I would tend to agree with you that you should have more responsibility than that in authority.

Mr. Secretary, as you know, one of my chief concerns is protection of critical infrastructure from cyber attack. I think all of us on this committee are aware of the threat that we face them in cyber space, and I am curious about your take on the response of critical infrastructure owners and operators. In my experience, there has been a tendency to meet the minimum requirements put on them, but to ask the Government to incentivize any measure taken beyond that. Do you believe owners and operators are innovating in their defensive efforts, or are they generally just getting by?

Secretary JOHNSON. I think it depends on the size of the business and the segment they are in, but I believe that owners and operators of critical infrastructure are taking the threat more and more significantly because of the information we are sharing with them about what we are seeing, about some of the threats that have been directed to them. So I believe there is an increasing awareness out there, and it is not just a minimalist approach.

Mr. LANGEVIN. Thank you.

Director Comey, in your testimony, you referenced the steps the FBI has taken to continue to gather intelligence to stop terrorism despite the challenge of Going Dark. I share your concern. Can you expand on this beyond working with tech companies to address the problem directly and acknowledging that you are not asking for a legislative solution. What are the other methods the FBI does employ?

Mr. COMEY. Thank you, Congressman.

We—when we face a needle that has gone invisible on us, we have to lean more heavily on traditionally law enforcement techniques, see if we can get a source close to the person, see if we can get an undercover close to the person, see if physical surveillance tells us something about the person, and those obviously—there is obvious shortcomings in those techniques, but we are not going to stop trying to get the job done. So we will just lean on other things we have done for years. It will be inadequate, frankly, but we will keep working at it.

Mr. LANGEVIN. I thank the Chair. This is an issue that I have increasing concern about, this going dark, and our intel and law enforcement's ability to really adequately see into the threats that are facing us. It is a challenge that we are going to have to continue to confront.

Chairman MCCAUL. Yeah. I share that concern, as well.

The Chair recognizes Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. Secretary, I share the concerns outlined by Mr. Smith about ISIL using the Syrian refugees that the President has decided to allowed into this country as a vehicle to sneak bad actors in.

You described a, "pretty thorough vetting process" as a part of your response to his answer. Can you tell me more about that process?

Secretary JOHNSON. Well, first of all, we are happy to brief you on the more sensitive aspects of it in a nonpublic setting. But it involves consulting a number of different agencies, law enforcement and intelligence, and the information that they have regarding each individual applicant.

It is a more robust process than it used to be. To some, it is time-consuming, but it is something that I think we need to do. It involves any information you may have. It may take some time to resolve any uncertainties about the information. Sometimes there may be a variance in a name or a date of birth or something of that nature. But it involves consulting a number of different agencies as well as a personal interview and gathering simply as much information as we possibly have about the person.

Mr. ROGERS. I would appreciate it if you would have your appropriate staff member schedule that brief for me in a SCIF and any other Members of the committee that would like to participate.

Director Comey, from personal experience, I have seen your agency do some phenomenal things with virtually no evidence, other than a bad act, to locate bad people.

Having said that, I am curious to know, is there any other tool that we can provide you, that the Congress could provide you, that would help you locate these individuals that you all referred to on social media that are recruiting and organizing in this country that you don't have at present?

Mr. COMEY. I don't think so, Congressman. To me, this conversation about going dark is not about new authorities for the FBI. You have given us the authority to go to Federal judges and make a showing of probable cause and get a search warrant or get an order to intercept communications. We think that is appropriate. We are big fans of the rule of law and the Bill of Rights, and so I think that is a good set of authorities.

The challenge we face is solving the problems where those tools under the Fourth Amendment are no longer as effective as they were before. That is this huge, knotty problem I am talking about.

So I don't see it as more authorities for the FBI. I see it as all of us together trying to figure out how the authorities we already have, the American people have given us, can be used to good effect.

Mr. ROGERS. You also made reference earlier, you and Secretary Johnson, about the surge of activity that you are having to manage now. Do you have the adequate resources to deal with that surge? I know Secretary Johnson has talked about sequestration and its burdens on his agency. What do you think about that? Do you have what you need?

Mr. COMEY. The honest answer is I don't know. For this reason, I say that: If what we experienced in May, June, and into the early part of July were to become the new normal, it would really stretch the FBI. Because, to meet that surge, we had to move a lot of folks from criminal work, because surveillance is only easy on TV. Following somebody 24/7 without them knowing you are there is really hard. So we had to surge hundreds of people from criminal cases, which are important, move them over to the National security side.

That bump in cases has dropped off a little bit, and so we are watching it very closely. We have moved people back to be able to do the criminal work. But if that surge becomes our new normal, then I will have a different view of it. I will obviously make sure Congress knows the minute I have reached that conclusion.

Mr. ROGERS. Well, I hope you will. We want to be helpful. We want to give you the tools that you need. But, frankly, we have to hear from you what you need. We can't help you unless you tell us what you need.

Mr. COMEY. Yes, sir.

Mr. ROGERS. Thank you. I yield back.

Chairman MCCAUL. Thank you.

The Chair recognizes Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman.

In light of the challenges that you described in terms of encryption and expanding social networking, I think one strategy is to maximize our other abilities to try and thwart terrorist acts. Along those lines, it has been a priority of mine, a priority of the committee's to look at enhancing information sharing among Federal agencies and local law enforcement, as well, particularly in the wake of the Boston Marathon bombing.

I know that the FBI has moved forward in this, and I know that DHS has offered recommendations in this regard that we are reviewing here.

If I could, you know, Director Comey, if you could just give us an update on what you have done already in the wake of the Boston Marathon bombing—use that as a time frame—and what you see going forward and any time lines in pursuing that.

Mr. COMEY. Yeah. Thank you, Congressman Keating.

I think we learned some good things for us to get better, coming out of the Boston Marathon bombing. I appreciate your focus on it and the committee's. I believe we are in a much better place today.

We can always be better, but here is how I think about our improvement.

We now make sure that everybody on the Joint Terrorism Task Force knows that our default is sharing information. In particular, we want the leaders of the agencies represented in our Joint Terrorism Task Forces to understand that and actually participate in it.

So we do an inventory review in each single JTTF on a regular basis. Sometimes it is once a week; sometimes it is once a month. We want everybody to come in and sit down and say, "This is the stuff we opened in the last month, this is the stuff we closed; questions, concerns, anybody want to follow up on it?" so they are engaged at the JTTF, but also, if there is something else they want to do in response to the inventory, they are able to do that.

So I think we have pushed that both in letter, which is important, but in spirit, which, frankly, is more important, to understand, everybody, we are in this together. Especially this threat that is so spread out, we need State and local partners to spot this and stop it.

So I think we are in a much better place than we were 2½ years ago. As I said, I don't want to be overconfident, though. There are always ways to find ways to improve, but that is my sense of where we are.

Mr. KEATING. I think all of your agencies have done an extraordinary job in thwarting so many potential terrorist threats. You have done a great job, if you use the analogy, of swatting mosquitoes, but the other thing we have to do, particularly in light of some of our challenges, is to dry up the swamp as much as we can.

Along those lines, I think it is very important work that DHS has done, the Office of Community Partnerships, and making that the hub, the central point of trying to thwart some of these attacks.

I would like to ask the Secretary—Secretary Johnson, what is your progress in that? How do you value that? How is your funding for that? Because I am concerned about some of that. If you could, I think it is promising that peer-to-peer—if you could explain to the committee your progress with the peer-to-peer program, how that might be working, because it is important.

We are a great country. No one, I don't think, has the resources to out-message us. But what we are not doing is we are not maximizing on that, and that is important.

So if you could comment on that, sir.

Secretary JOHNSON. Thank you for that question.

I have taken a great personal interest in countering violent extremism. I believe it is fundamental and indispensable to our overall efforts. So I have done a number of community engagements myself.

The reason I created the Office for Community Partnerships is because I think we need to take our efforts to the next level. So what this office does is consolidate in one place all the people across my Department that are devoted to our CVE efforts. I want to build on that so that we have a field capability. I want an office that will, in addition to engaging the community, also engage the tech sector, engage philanthropies, develop our own grant-making capabilities here.

In terms of adequate funding, the single biggest thing that I am going to keep coming back to in terms of adequacy of funding is: Please repeal sequestration. If I have to deal with sequestration, then I come up short on CVE and a lot of other things.

Mr. KEATING. How about peer-to-peer, the peer-to-peer program? Are we engaging young people in terms of this messaging process? Could you comment on that briefly?

Secretary JOHNSON. I think that among bright, college-age people in particular lie the best ideas on CVE for the way forward. So I have engaged several college organizations on helping us in our efforts. That is a work in progress.

In my experience, young people, college-age people tend to approach CVE a little differently than older, more experienced people of their parents' age, which I can talk with you at greater detail off-line about.

Mr. KEATING. Yeah.

Lastly, just a comment that the perimeters that your agencies have are important. That is why you are here. But if we are going to be successful, we are going to have to expand out beyond that, in the non-profit side, the public side, the private side, and obtain more engagement. So I think that we shouldn't shortchange resources that all your agencies have to try and do that, as well, because I think it is an important aspect, and it is one that we still haven't maximized.

Thank you, and I yield back.

Chairman MCCAUL. Thank you.

I want to commend the Secretary for adopting a lot of the provisions in the combating violent extremism bill we marked up out of committee. We appreciate that.

The Chair recognizes Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman.

Secretary Johnson, the term "OTM," "Other than Mexicans," is a DHS term, correct?

Secretary JOHNSON. It is certainly a term we use around DHS.

Mr. DUNCAN. Used by your field officers of people apprehended crossing the Southern Border that are not of Mexican descent.

Secretary JOHNSON. Yes.

Mr. DUNCAN. Okay.

I am going to take all Latinos out—Guatemalans, Hondurans, El Salvadorans, all those out. There are other people that cross the border that are of African, Asian, and Middle Eastern descent. Am I not correct?

Secretary JOHNSON. You are correct.

Mr. DUNCAN. That are apprehended crossing the Southern Border.

Secretary JOHNSON. Yes.

Mr. DUNCAN. Okay. Thank you.

Secretary JOHNSON. You are absolutely correct.

Mr. DUNCAN. Well, our Southern Border is not secure. We have no idea who is coming into this country. I could go on to Iran and Hezbollah and the tri-border region and the ties between Lebanon and Paraguay, the tri-border region there that the Chairman and I investigated a number of years ago. But let me shift.

We have no idea who is in this country. We have no idea who can come into this country through our Southern Border, because it is not secure.

Are you familiar with the Jewish museum that was shot up in Brussels in, I think, May or June 2014?

Secretary JOHNSON. Yes.

Mr. DUNCAN. Okay. That is for Director Comey, too.

Several people died. The perpetrator was a foreign fighter who had been trained in Libya or Syria or Iraq; we are not sure. But he made his way back into Europe. And because of Schengen and open borders, he made his way to Brussels and killed several people and then fled. Made it all the way to Marseilles, France; was just about to jump out of Europe into Africa before he was apprehended.

These are the facts. Foreign-fighter flow is something we have to be very, very serious about, especially because of open borders, especially because of the millions of middle-age and young Middle Eastern men that have migrated to Europe who could possibly have the ability to enter in this country because of open borders, visa waiver programs. It may not be this year, it may be 5 years after they get citizenship, whatever it takes.

I will say this. I think the Chairman misspoke a while ago when he used the number of 10,000 immigrants coming into this country, refugees in the resettlement program. I have heard the number is 100,000 next year. Regardless, it is too many if we do not have the ability to properly vet those individuals.

Some of those will come to South Carolina. I will tell you that the folks in South Carolina are very, very concerned about our inability to vet properly the refugees that are coming.

I have been to the refugee camp in Jordan. I understand the immense challenge that we face from a humanitarian standpoint. I understand the need or desire for folks to leave the Middle East and travel to Europe or try to come to this country to try to create a better life for their family. I think the Chairman spoke appropriately when he said we are a very humanitarian Nation. History proves that.

But we have a different situation on our hands. We have a group known as ISIS—and al-Qaeda is still relevant in this world as a threat to the United States—who want to come to this country, who have said they will exploit this refugee program to come to this country. If they are able to make it to Europe and they are able to jump to Africa and make it to South America or Latin America, because of our open borders issues, they could come across our border the way the OTMs are coming today.

So, Mr. Comey, what can I tell folks in South Carolina about our vetting of these refugees that will put their minds to rest that we are properly vetting everyone that may come into my State that may wish to harm the United States? What can I tell them? Please share with me some bit of good news about this Refugee Resettlement Program, because I am not hearing it.

Mr. COMEY. The good news is we are much better at doing it than we were 8 years ago. The bad news is there is no risk-free process.

Mr. DUNCAN. So I hear interviews in the camps, in the refugee camps, but I also hear that the records aren't there. So I just want to encourage you all, the three of you that are charged with the National security of this country, to rethink the resettlement of refugees in this country, especially in the numbers that I am hearing.

With that, Mr. Chairman, I yield back.

Chairman MCCAUL. And——

Secretary JOHNSON. Mr. Chairman, can I——

Chairman MCCAUL. Yeah, a point of clarification. I think it is important, and I think that is where you are going, because the public have thrown out the 100,000 number as Syrian refugees. My understanding is that there are 100,000 refugees total world-wide and 10,000 potentially from Syria, and maybe you want to clarify that.

Secretary JOHNSON. What we have said is that, for fiscal year 2016, we will commit to resettling 10,000 Syrian refugees and a total world-wide of 85,000.

Chairman MCCAUL. Okay. I just wanted to get that on the record while we——

Mr. DUNCAN. Well, Mr. Chairman, if I may, where do we anticipate those 85,000 coming from? Syria? Iraq? Afghanistan? Libya? Do we have any idea? Can we identify the countries that are being targeted for refugee resettlement?

Secretary JOHNSON. Well, it is done by regions of the world, sir. That is a publicly-available fact, which we can get you. But refugees tend to come from every part of the world, obviously, some more troubled places than others.

Mr. DUNCAN. Okay.

Thank you, Mr. Chairman.

Chairman MCCAUL. Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman, and thank you for holding this hearing.

Thank you, gentlemen.

I tell you, it is actually comforting to hear you refer to each other by first name. It means you are collaborating and cooperating. It is good that there is a relationship there. It makes me feel a little bit better, although this is a very scary time.

I have a few questions. I want to start with a question with you, Mr. Johnson. The United States Secret Service is leading an investigation of an on-line hacker that recently told *The Washington Post* he gained access to not only the CIA director's personal email account but also to your own email account.

Would you please describe what current plan is in place for the Secret Service to prevent this intrusion, given the external infiltrations the Department has experienced recently, including the OPM data breach?

Secretary JOHNSON. Ma'am, I don't think that I can comment about an on-going investigation. The one thing I will say is don't believe everything you read in the newspaper because a lot of it is inaccurate. But there is a pending investigation by the FBI and the Secret Service, and so I don't think I can comment right now.

Mrs. WATSON COLEMAN. Okay. Thank you.

I am very interested in how we are approaching and looking at the security and safety threats to us, obviously, by those who are influenced or directed by foreign countries and jihadists but also

those who are our own home-grown, right-wing extremists who wreak dangerous conditions upon unsuspecting, innocent people.

So I would like to know from the three of you whether or not there is an assessment of a greater risk or equal risk or lower risk from one type of violent experience as opposed to the other and what kind of resource application we have across the various entities that deal with both types, both the, sort-of, right-wing extremists——

Mr. COMEY. All right.

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

Mr. COMEY. There are two parts to the FBI's Counterterrorism Division: International terrorism, domestic terrorism.

We have hundreds and hundreds of people wake up every day worrying about domestic extremists. By that, I mean people who are not inspired or motivated by international terrorism organizations but are people who see themselves as part of some political resistance movement or some racially motivated movement in the United States. So we do a lot of work on that front.

Our assessment of the threat is it is about the same as it was over the last couple of years, hasn't dropped. It is about the same.

The international terrorism threat, with respect to both that coming from the outside in and those motivated internally, as we have discussed here today, has changed and gone up, especially with those who are responding to ISIL's twin-pronged message.

Mrs. WATSON COLEMAN. So, for clarification purposes, though, is there any sort of ranking between the two types of violence?

Mr. COMEY. There is not.

Mrs. WATSON COLEMAN. Is there a greater threat from the domestic right-wing extremist who is racist and anti-Semitic and all those things as opposed to the jihadist-inspired or -directed?

Mr. COMEY. We do not compare them in that way. That is sort of like, which do you dislike more, heart attacks or cancer? They are both——

Mrs. WATSON COLEMAN. Do you have to consider——

Mr. COMEY [continuing]. Very dangerous things——

Mrs. WATSON COLEMAN. But do you——

Mr. COMEY [continuing]. We focus——

Mrs. WATSON COLEMAN. I am sorry.

Mr. COMEY. Sorry.

Mrs. WATSON COLEMAN. I am just trying to get at, is there a difference in the application of resources for one type versus the other? Are there different offices in charge of one type or the other, or is there sort of a cross-pollination?

Mr. COMEY. Well, there are, as I said, two divisions in the FBI's Counterterrorism Division. One focuses on the domestic terrorist threat, and the other focuses on the international, including its manifestations inside the country.

Then they talk to each other a lot. I have gotten briefings from them jointly, because they worry about whether there is any kind of crossover.

But we think about them using the same kind of intelligence resources. We apply the same tools to understand presence on social media. So we are addressing both as the serious threats that they are.

Mrs. WATSON COLEMAN. Are we collecting information on the type of violence that occurs, like that occurred at Mother Bethel Church and around the country? Are we collecting that data and putting that into a database and sharing that so we have an understanding of those types of violent extremists?

Mr. COMEY. Yes.

Mrs. WATSON COLEMAN. Thank you.

Mr. Johnson and Mr. Rasmussen, do you care to comment on that at all?

Secretary JOHNSON. I don't think there is anything I can add to what Jim said.

Mrs. WATSON COLEMAN. Okay.

Mr. RASMUSSEN. I agree. Actually, my mission area actually leaves me outside of the domestic terrorism, except for analytical purpose.

Mrs. WATSON COLEMAN. Uh-huh.

My last question is a really, really quick one. I wasn't here—and I don't think you either were here—but do we have knowledge on whether or not we have had the same kind of angst and anxiety when there was resettlement from the Iraqi refugees? Do we find that that angst has been addressed? Have we found learned lessons and done things differently? Thank you.

Thank you, Mr. Chair.

Secretary JOHNSON. The short answer is, yes, we have. There have been lessons learned from the Iraqi refugee experience which I believe have, and I think with the FBI, improved the process.

Mrs. WATSON COLEMAN. Thank you very much.

Thank you, Mr. Chairman.

Chairman MCCAUL. The Chair recognizes Mr. Clawson.

Mr. CLAWSON. Thank you, Chairman, for your leadership here today, as always.

Appreciate all three of you all coming today and what you do for our country and the sacrifice you make, because it is not small. So I appreciate that.

On a personal level, I get tired of the bad trade deals that our country makes. I get tired of our trading partners taking us to the cleaners. I get tired of good-paying American manufacturing jobs going overseas. Like this morning, if I am the UAW, I am not happy with the Chinese currency and their export subsidies. If I am Harley-Davidson, I am probably not happy with where the yen is today, as we see our American manufacturing infrastructure get decimated. Pretty soon, we are just not going to make anything anymore. What is wrong—why not protect the American worker a little bit?

On top of that, the Chinese hack us. Wait a minute. Billions of dollars every month go to the Chinese in a trade deficit. They hack our companies, and they hack our Government. We just keep on trading.

Now, as I understand it, Secretary Johnson, you said time will tell whether what we have done will keep them from hacking in the future. I say, why don't we protect the American worker, the American company, American unions, the UAW, and our infrastructure at the same time? Because if we put our markets on the table and said, "Any more hacking, you lose access to our retail

markets," that would go away immediately, because they depend on us to live.

So, while I watch our manufacturing sector get decimated and these folks hacking us, you are there with the administration. I just wonder why we don't use the obvious leverage that we have. It is obvious. It makes me upset because I see so many of my friends and people I grew up with lose good-paying American jobs.

You say only time will tell whether the Chinese are going to obey us or not or cooperate or not, while we open up our markets. Am I missing something on my analysis of this situation, Secretary?

Secretary JOHNSON. In response to the cyber attacks on our Government and on the private sector, there are a number of things, seen and unseen, that we have done and that we are considering.

What I was referring to—what I am referring to when I said time will tell, when the president of China was here and in the run-up to his visit, the Chinese Government agreed that economic espionage and theft of commercial information for commercial purposes was wrong and was a crime. They agreed to that in writing. Time will tell whether they will live up to that agreement. But it was significant, in the sense that they publicly, out of the mouth of their President, committed to that. But time will tell whether——

Mr. CLAWSON. Have we ever talked, has the leadership of our country, of using the obvious market leverage that we have—as almost a third of the global GDP and the source of economic growth for the whole world, do we ever talk about using that leverage to get not only fair trade deals but keep them from robbing our IP and keep them from hacking?

I mean, we could stop it next month. Just shut down the retail markets to cheaters, and let the American worker catch a break for once, all at the same time.

Secretary JOHNSON. I would have to refer you to other agencies of our Government about that.

Mr. CLAWSON. But, look, you are part of the leadership structure. Excuse me, but you are on the board of directors, you are in the staff meetings, you know, and part of this touches you. I think if you were back in the private sector at a board of directors meeting, that answer might not be acceptable.

I am asking, does the senior leadership of our country, as we get taken to the cleaners on trade and on hacking and on IP, has anybody thought about using our markets as leverage? Do you all talk about that?

Secretary JOHNSON. I suspect the answer is yes——

Mr. CLAWSON. Well, then I would like to see a little bit.

Secretary JOHNSON [continuing]. But I, again, refer you to other agencies of our Government——

Mr. CLAWSON. Come on now.

Secretary JOHNSON [continuing]. That can give you an answer to that question.

Mr. CLAWSON. You know, the American worker doesn't want referring to other agencies. Our folks that get their technology stolen don't want to get referred to other agencies. They want leadership. We are getting taken to the cleaners on four different fronts, and we don't want to get referred to an outside study. We want leader-

ship for American jobs and American technology. I don't think that is too much to ask.

You are part of the team. Help our companies and help our unions and our workers get a fair shake.

I yield back.

Chairman MCCAUL. The Chair recognizes Ms. Jackson Lee.

Ms. JACKSON LEE. Good morning. I thank the Chairman very much and the Ranking Member for these important hearings on protecting the American people.

I want to pursue a line of questioning that sort-of follows the opening statements that you gentlemen have made.

I take from the director of the National Counterterrorism Center his sentence that said, "The array of extremist terrorist actors around the globe is broader, wider, and deeper than it has been at any time since 9/11, and the threat landscape is less predictable." I think that is an important sentence that has been really crafted and reinforced by the testimony and the leadership of all three of you. I appreciate your service very much.

I have introduced the No Fly for Foreign Terrorists. I would like to pursue, and starting with Director Comey, to reinforce the seriousness with which we should take, even though there is a lot of work, of individuals leaving the United States and potentially coming back to the United States, having gone to be part of the caliphate or ISIL, and to come back to the United States.

Can you frame again how extensive that threat is?

Mr. COMEY. Well, the returning terrorist fighter threat is what I understand you to be asking about—is one that we are watching very closely today. We see the logic of it telling us that is going to be a problem for the next 5-years-plus. Because not every terrorist is going to get killed on the battlefield in Syria or Iraq, so, inevitably, there will be a terrorist diaspora out of the so-called caliphate to Western Europe or to the United States.

So it is a threat that all three of us and the people we represent think about every day and also think about how it is going to manifest down the road.

Ms. JACKSON LEE. Do you maintain a statement that you made a couple of weeks ago, that there is a terrorist cell in almost—I think you said almost 50 or all 50 States that the FBI is aware of?

Mr. COMEY. In all 50 States, we have open terrorism investigations related to a number of dimensions of the threat. But in all 50 States, we have ISIL radicalization cases under investigation.

Ms. JACKSON LEE. I understood you also to be a supporter of the concept of collecting data. I serve on another committee dealing with crime and terrorism and investigations. My understanding is that you believe that we should be in the business of ensuring the data is collected sufficient for information on how to act on some of these issues of terrorism in particular.

Mr. COMEY. I do. I am a big supporter of the rule of law and using it to collect the information that will help us keep people safe.

Ms. JACKSON LEE. I am very glad that you said that. I would like to add into the—when I say that, the rule of law. Thank you. Because I think that is an important point that people are concerned about.

But I would like to put into the record the No Fly for Foreign Fighters. I ask unanimous consent, Mr. Chairman.

Chairman MCCAUL. Without objection, so ordered.*

Ms. JACKSON LEE. Thank you very much.

To the Secretary, let me first of all indicate that we are certainly concerned about the hacking incident. I realize that it is under investigation. I would ask this committee that we would have an opportunity for a Classified briefing. I, frankly, apologize for you, a public servant, to have had that issue occur.

But let me move forward to this issue of the power grid and cybersecurity, which I believe you have indicated that we need more legislation. You also indicated that we should get rid of sequester. Let me say that I support you, and many of us do. It is very hard to function.

But I also would like to hear your comment about the power grid of the United States and the work that the Homeland Security Department is doing, the framework it is doing. I would like to commend you to some legislation that I am going to offer into the record regarding focusing specifically on the power grids of the United States.

Would you just respond to that?

I would also like the director of counterterrorism to, as well, answer that and follow up by answering a question regarding the handle that we have on Syrian refugees that may be coming into the United States.

I want to thank the Secretary for coming to my district and having a very productive meeting with Syrian Americans, Syrians in Houston who are open and welcoming those who may have to come out of persecution.

Secretary.

Secretary JOHNSON. With regard to cybersecurity, the two most significant things that we are hoping and need from Congress are provisions in law to encourage the private sector to share information with my department, cyber threat indicator information with my department. Sharing information is vital to our homeland security efforts for the private sector and for the Government sector.

The other thing that is in pending legislation in now the House and Senate is something that explicitly authorizes the system we have for detecting, monitoring, and blocking unwanted intrusions, what is currently our EINSTEIN system.

So those are two things in pending legislation that I think would be extremely helpful to our overall cybersecurity efforts.

Ms. JACKSON LEE. Do you believe that—first of all, the idea of the cybersecurity issue is that a lot of the infrastructure is in the private sector. Is there enough collaboration with the private sector? When we think of power, we also think of water and other elements that serve the public. Is there enough of an element of collaboration to be able to put up that firewall protecting a potential cyber threat or cyberterrorism?

Secretary JOHNSON. There is not enough, and so we need to encourage more.

---

*The information has been retained in committee files. H.R. 48, 114th Congress, the "No Fly for Foreign Fighters Act" is available at *http://www.congress.gov/bill/114th-Congress/house-bill/48*.

Ms. JACKSON LEE. Thank you.

Mr. Rasmussen, would you answer the question?

Mr. RASMUSSEN. To your question, ma'am, on the degree to which terrorist organizations are interested in developing a cyber capability, they absolutely are. It is clearly a growth industry as far as terrorist organizations are concerned, and particularly ISIL.

Thus far, the capability seems to be more evident at, I would say, the low end of the spectrum. I don't mean "low" in terms of minimizing, but, thus far, the kind of capability we have seen largely shows up in terms of pushing out people's personal information in a public way, which is potentially very destructive.

Their interest in attacking in a cyber way our electrical power grid or other forms of critical infrastructure we have, thus far we see that as more aspirational, not something where we see capability actually existing. But believe me, it is something we are very, very carefully watching, because it is a way for a terrorist group to try to achieve wide-spread impact.

Ms. JACKSON LEE. Well, as I ask the Chairman if I could put these items into the record, let me just say that we know that a number of terrorist incidents were aspirational 1, 2 years ago. I can't emphasize enough my concern on the cyber attack of the Nation's power grid. I don't think we are putting any extra information out. I hope that all of you will focus very pointedly on that as a major concern.

Mr. Chairman, I would like to—and thank you very much for your testimony—yield back, but I would like to ask the Chairman to allow me to put into the record an article from *The Hill* regarding "Pushing to Boost Power Grid Defenses Against ISIS" and also a CNN statement regarding "ISIL Is Beginning To Perpetrate Cyber Attacks." I ask unanimous consent for the record.

Chairman MCCAUL. Without objection.

[The information follows:]

ARTICLE SUBMITTED FOR THE RECORD BY HON. SHEILA JACKSON LEE

OCTOBER 19, 2015, *The Hill*

JACKSON LEE PUSHES TO BOOST POWER-GRID DEFENSES AGAINST ISIS

By Katie Bo Williams—10/19/15 09:38 AM EDT

Rep. Sheila Jackson Lee (D–Texas) on Friday called for action on a bill bolstering power-grid cybersecurity after a Department of Homeland Security (DHS) official said the Islamic State in Iraq and Syria (ISIS) is trying to hack American electrical power companies.

"No solace should be taken in the fact that ISIS has been unsuccessful," Jackson Lee said. "ISIS need only be successful once to have catastrophic impact on regional electricity supply."

Caitlin Durkovich, assistant secretary for infrastructure protection at DHS, told energy firm executives at an industry conference in Philadelphia last week that ISIS "is beginning to perpetrate cyberattacks."

Law enforcement officials speaking at the same event indicated that the group's efforts have so far been unsuccessful, thanks in part to a Balkanized power grid and an unsophisticated approach.

"Strong intent. Thankfully, low capability," said John Riggi, a section chief at the FBI's cyber division. "But the concern is that they'll buy that capability."

Jackson Lee, a senior member of the House Homeland Security Committee and ranking member on the Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, in January introduced the Terrorism Prevention and Critical Infrastructure Protection Act.

The bill directs DHS to work with critical infrastructure companies to boost their cyber defenses against terrorist attacks, part of a swath of legislation that has attempted to codify the agency's responsibilities in that area.

Late last year, the Senate passed its version of the House-passed National Cybersecurity and Critical Infrastructure Protection Act.

The bill officially authorized an already-existing cybersecurity information-sharing hub at DHS.

Although a deadly attack on power plants or the electric grid—a "cyber Pearl Harbor"—is still only a hypothetical, experts warn critical infrastructure sites are increasingly at risk, as electric grids get smarter.

National Security Agency Director Michael Rogers told lawmakers last fall that China and "one or two" other countries would be able to shut down portions of critical U.S. infrastructure with a cyber attack. Researchers suspect Iran to be on that list.

In August, DHS announced the creation of a new subcommittee dedicated to preventing attacks on the power grid.

The new panel is tasked with identifying how well the department's lifeline sectors are prepared to meet threats and recover from a significant cyber event.

The committee will also provide recommendations for a more unified approach to state and local cybersecurity.

"There is a great deal that has been done and is being done now to secure our networks," Homeland Security Secretary Jeh Johnson told the House Judiciary Committee in July. "There is more to do."

STORY SUBMITTED FOR THE RECORD BY HON. SHEILA JACKSON LEE

CNN: ISIS is attacking the U.S. energy grid

October 15, 2015

The Islamic State is trying to hack American electrical power companies—but they are terrible at it.

U.S. law enforcement officials revealed the hack attempts on Wednesday at a conference of American energy firms who were meeting about national security concerns.

"ISIL is beginning to perpetrate cyber attacks," Caitlin Durkovich, assistant secretary for infrastructure protection at the Department of Homeland Security, told company executives.

Investigators would not reveal any details to CNNMoney—or cite evidence of specific incidents.

But they did say the attacks by the Islamic State have been unsuccessful. Terrorists are not currently using the most sophisticated hacking tools to break into computer systems and turn off or blow up machines.

"Strong intent. Thankfully, low capability," said John Riggi, a section chief at the FBI's cyber division. "But the concern is that they'll buy that capability."

Indeed, hacking software is up for sale in black markets on-line. That's often how mafias acquire the cyber weapons they use to break into companies and steal giant databases of information they later sell to fraudsters.

The FBI now worries that the Islamic State or its supporters will buy malicious software that can sneak into computers and destroy electronics. An attack on power companies could disrupt the flow of energy to U.S. homes and businesses.

And it's not just Islamic extremists. There's an equal threat from domestic terrorists and hate groups, according to Mark Lemery. He's the "critical infrastructure protection coordinator" who helps coordinate defenses against attacks in Utah. But again, the worries are tempered.

"They'd love to do damage, but they just don't have the capability," Lemery said. "Terrorists have not gotten to the point where they're causing physical damage."

Officials made clear that the greater concern is attacks from other countries. Riggi said malware found last year on industrial control systems at energy companies—including pumps and engines—were traced to the Russian government.

Besides, the likelihood of a hack taking out the entire U.S. energy grid—or even a section of it—is extremely low. The grid isn't as uniform and connected as people might believe. Currently, it's a chaotic patchwork of "grids," each with different types of machines and software that don't smoothly coordinate or communicate.

That jumble actually works to the nation's advantage, energy company executives said. It would take a large, expensive team of highly technical spies to understand the layout of computers and machines at an energy company. Then it takes stellar hackers to sneak in. And even if they do manage to flip a switch—which companies

maintain has never happened here in the United States—the attack might only take out electricity fed to a tiny portion of land, maybe a section of a city. An entirely different type of attack would be needed to carry that over to the next power plant.

Experts attending GridSecCon, held by the North American Electric Reliability Corporation, seemed cautious but hopeful.

When energy industry representatives asked Riggi how the FBI knows who's hacking—whether it's a government or independent hacking group—he said American spies that are monitoring computer networks are quick to share information with law enforcement.

"We've had pretty good success actually," Riggi said. "Since the FBI is an intelligence agency, we rely on the help of CIA and NSA. We compare information with the NSA."

Ms. JACKSON LEE. And to put into the record H.R. 85, I ask unanimous consent.

Chairman MCCAUL. Without objection.**

Ms. JACKSON LEE. And ask to put into the record a letter to the President on encryption signed by over 100 individuals who are very concerned about any proposals that we don't oversee—even though I want to give tools appropriately—oversee in the right way to protect both the American people and follow the rule of law. I ask unanimous consent.

Chairman MCCAUL. Without objection.

[The information follows:]

LETTER SUBMITTED FOR THE RECORD BY HON. SHEILA JACKSON LEE

May 19, 2015.

President BARACK OBAMA,
The White House, 1600 Pennsylvania Avenue NW, Washington, DC 20500.

DEAR PRESIDENT OBAMA: We the undersigned represent a wide variety of civil society organizations dedicated to protecting civil liberties, human rights, and innovation on-line, as well as technology companies, trade associations, and security and policy experts. We are writing today to respond to recent statements by some Administration officials regarding the deployment of strong encryption technology in the devices and services offered by the U.S. technology industry. Those officials have suggested that American companies should refrain from providing any products that are secured by encryption, unless those companies also weaken their security in order to maintain the capability to decrypt their customers' data at the government's request. Some officials have gone so far as to suggest that Congress should act to ban such products or mandate such capabilities.

We urge you to reject any proposal that U.S. companies deliberately weaken the security of their products. We request that the White House instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology. Such policies will in turn help to promote and protect cybersecurity, economic growth, and human rights, both here and abroad.

Strong encryption is the cornerstone of the modern information economy's security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, repressive governments trying to stifle dissent, or foreign intelligence agencies trying to compromise our and our allies' most sensitive national security secrets.

Encryption thereby protects us from innumerable criminal and national security threats. This protection would be undermined by the mandatory insertion of any new vulnerabilities into encrypted devices and services. Whether you call them "front doors" or "back doors", introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government's own experts.

** The information has been retained in committee files. H.R. 85, 114th Congress, the "Terrorism Prevention and Critical Infrastructure Protection Act of 2015" is available at *http://www.congress.gov/bill/114th-Congress/house-bill/85*.

In addition to undermining cybersecurity, any kind of vulnerability mandate would also seriously undermine our economic security. U.S. companies are already struggling to maintain international trust in the wake of revelations about the National Security Agency's surveillance programs. Introducing mandatory vulnerabilities into American products would further push many customers—be they domestic or international, individual or institutional—to turn away from those compromised products and services. Instead, they—and many of the bad actors whose behavior the government is hoping to impact—will simply rely on encrypted offerings from foreign providers, or avail themselves of the wide range of free and open source encryption products that are easily available on-line.

More than undermining every American's cybersecurity and the nation's economic security, introducing new vulnerabilities to weaken encrypted products in the U.S. would also undermine human rights and information security around the globe. If American companies maintain the ability to unlock their customers' data and devices on request, governments other than the United States will demand the same access, and will also be emboldened to demand the same capability from their native companies. The U.S. government, having made the same demands, will have little room to object. The result will be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes. That's not a future that the American people or the people of the world deserve.

The Administration faces a critical choice: will it adopt policies that foster a global digital ecosystem that is more secure, or less? That choice may well define the future of the Internet in the 21st century. When faced with a similar choice at the end of the last century, during the so-called "Crypto Wars", U.S. policymakers weighed many of the same concerns and arguments that have been raised in the current debate, and correctly concluded that the serious costs of undermining encryption technology outweighed the purported benefits. So too did the President's Review Group on Intelligence and Communications Technologies, who unanimously recommended in their December 2013 report that the U.S. Government should "(1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge U.S. companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

We urge the Administration to follow the Review Group's recommendation and adopt policies that promote rather than undermine the widespread adoption of strong encryption technologies, and by doing so help lead the way to a more secure, prosperous, and rights-respecting future for America and for the world.

Thank you,

Civil Society Organizations

Access
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee (ADC)
American Civil Liberties Union
American Library Association
Benetech
Bill of Rights Defense Committee
Center for Democracy & Technology Committee to Protect Journalists
The Constitution Project
Constitutional Alliance
Council on American-Islamic Relations
Demand Progress
Defending Dissent Foundation
DownsizeDC.org, Inc.
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Engine
Fight for the Future
Free Press
Free Software Foundation
Freedom of the Press Foundation
GNOME Foundation
Human Rights Watch
The Media Consortium
New America's Open Technology Institute
Niskanen Center

Open Source Initiative
PEN American Center
Project Censored/Media Freedom Foundation
R Street
Reporters Committee for Freedom of the Press
TechFreedom
The Tor Project
U.S. Public Policy Council of Association for Computing Machinery
World Privacy Forum
X-Lab

Companies & Trade Associations

ACT/The App Association
Adobe
Apple Inc.
The Application Developers Alliance
Automattic
Blockstream
Cisco Systems
Coinbase
Cloud Linux Inc.
CloudFlare
Computer & Communications Industry Association
Consumer Electronics Association (CEA)
Context Relevant
The Copia Institute
CREDO Mobile
Data Foundry
Dropbox
Evernote
Facebook
Gandi.net
Golden Frog
Google
HackerOne
Hackers/Founders
Hewlett-Packard Company
Internet Archive
The Internet Association
Internet Infrastructure Coalition (i2Coalition)
Level 3 Communications
LinkedIn
Microsoft
Misk.com
Mozilla
Open Spectrum Inc.
Rackspace
Rapid7
Reform Government Surveillance
Sonic
ServInt
Silent Circle
Slack Technologies, Inc.
Symantec
Tech Assets Inc.
TechNet
Tumblr
Twitter
Wikimedia Foundation
Yahoo

*Security and Policy Experts**

Hal Abelson, Professor of Computer Science and Engineering, Massachusetts Institute of Technology
Ben Adida, VP Engineering, Clever Inc.
Jacob Appelbaum, The Tor Project

---

*Affiliations provided only for identification purposes.

Adam Back, PhD, Inventor, HashCash, Co-Founder & President, Blockstream
Alvaro Bedoya, Executive Director, Center on Privacy & Technology at Georgetown Law
Brian Behlendorf, Open Source software pioneer
Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University
Matt Bishop, Professor of Computer Science, University of California at Davis
Matthew Blaze, Director, Distributed Systems Laboratory, University of Pennsylvania
Dan Boneh, Professor of Computer Science and Electrical Engineering at Stanford University
Eric Burger, Research Professor of Computer Science and Director, Security and Software Engineering Research Center (Georgetown), Georgetown University
Jon Callas, CTO, Silent Circle
L. Jean Camp, Professor of Informatics, Indiana University
Richard A. Clarke, Chairman, Good Harbor Security Risk Management
Gabriella Coleman, Wolfe Chair in Scientific and Technological Literacy, McGill University
Whitfield Diffie, Dr. Sc. Techn., Center for International Security and Cooperation, Stanford University
David Evans, Professor of Computer Science, University of Virginia
David J. Farber, Alfred Filter Moore Professor Emeritus of Telecommunications, University of Pennsylvania
Dan Farmer, Security Consultant and Researcher, Vicious Fishes Consulting
Rik Farrow, Internet Security
Joan Feigenbaum, Department Chair and Grace Murray Hopper Professor of Computer Science Yale University
Richard Forno, Jr. Affiliate Scholar, Stanford Law School Center for Internet and Society
Alex Fowler, Co-Founder & SVP, Blockstream
Jim Fruchterman, Founder and CEO, Benetech
Daniel Kahn Gillmor, ACLU Staff Technologist
Robert Graham, creator of BlackICE, sidejacking, and masscan
Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society
Matthew D. Green, Assistant Research Professor, Johns Hopkins University Information Security Institute
Robert Hansen, Vice President of Labs at WhiteHat Security
Lance Hoffman, Director, George Washington University, Cyber Security Policy and Research Institute
Marcia Hofmann, Law Office of Marcia Hofmann
Nadim Kobeissi, PhD Researcher, INRIA
Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology
Nadia Heninger, Assistant Professor, Department of Computer and Information Science, University of Pennsylvania
David S. Isenberg, Producer, Freedom 2 Connect
Douglas W. Jones, Department of Computer Science, University of Iowa
Susan Landau, Worcester Polytechnic Institute
Gordon Fyodor Lyon, Founder, Nmap Security Scanner Project
Aaron Massey, Postdoctoral Fellow, School of Interactive Computing, Georgia Institute of Technology
Jonathan Mayer, Graduate Fellow, Stanford University
Jeff Moss, Founder, DEF CON and Black Hat security conferences
Peter G. Neumann, Senior Principal Scientist, SRI International Computer Science Lab, Moderator of the ACM Risks Forum
Ken Pfeil, former CISO at Pioneer Investments
Ronald L. Rivest, Vannevar Bush Professor, Massachusetts Institute of Technology
Paul Rosenzweig, Professorial Lecturer in Law, George Washington University School of Law
Jeffrey I. Schiller, Area Director for Security, Internet Engineering Task Force (1994–2003), Massachusetts Institute of Technology
Bruce Schneier, Fellow, Berkman Center for Internet and Society, Harvard Law School
Micah Sherr, Assistant Professor of Computer Science, Georgetown University
Adam Shostack, author, "Threat Modeling: Designing for Security"
Eugene H. Spafford, CERIAS Executive Director, Purdue University
Alex Stamos, CISO, Yahoo

Geoffrey R. Stone, Edward H. Levi Distinguished Service Professor of Law, The University of Chicago
Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology
C. Thomas (Space Rogue), Security Strategist, Tenable Network Security
Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute of Public Policy
Nicholas Weaver, Researcher, International Computer Science Institute
Chris Wysopal, Co-Founder and CTO, Veracode, Inc.
Philip Zimmermann, Chief Scientist and Co-Founder, Silent Circle

Ms. JACKSON LEE. I have two——

Chairman MCCAUL. How many more do you have?

Ms. JACKSON LEE. Just two more.

Chairman MCCAUL. Okay.

Ms. JACKSON LEE. A United States of America report on refugee resettlement and also "Analysis by Top Computer Experts on Encryption."*** I ask unanimous consent.

Chairman MCCAUL. Without objection.

[The information follows:]

SUBMITTED FOR THE RECORD BY HONORABLE SHEILA JACKSON LEE

UNHCR RESETTLEMENT HANDBOOK—COUNTRY CHAPTERS

COUNTRY CHAPTER USA: THE UNITED STATES OF AMERICA

By The Government of the United States of America, July 2011, revised October 2014

UNITED STATES OVERVIEW		
Resettlement programme since: 1975.	Selection Missions: Yes	Dossier Submissions: No
Resettlement Admission Targets:	2013–2014 ..... 1 Oct 2013–30 Sept 2014	2014–2015 1 Oct 2014–30 Sept 2015
Admission targets for UNHCR submissions:	52,300	56,000
Target for non-UNHCR submissions:	17,700	14,000
Total Resettlement Admission Target:	70,000	70,000

REGIONAL ALLOCATIONS (1 OCTOBER–30 SEPTEMBER)

Region	2013–2014		2014–2015	
	UNHCR	Non-UNHCR	UNHCR	Non-UNHCR
Africa	15,000	0	16,500	500
East Asia	14,000	0	12,800	200
Europe/Central Asia	0	1,000	0	1,000
Americas	300	4,700	700	3,300
Near East/South Asia	21,000	12,000	24,000	9,000
Allocated from Reserve	2,000	0	2,000	0
Total	52,300	17,700	56,000	14,000

***The information has been retained in committee files, entitled "Computer Science and Artificial Intelligence Laboratory Technical Report", and is available at *http://hdl.handle.net/1721.1/97690.*

SUB-QUOTA FEATURES

Designated Sub-Quota/Acceptance For	Description, Additional Comments
Emergency resettlement procedures	No specific quota. Very limited capacity to process applicants from referral to arrival in approx. 16 weeks.
Medical cases	No limits on submissions.
Women-at-risk cases	No specific quota.
Unaccompanied children	Accepted with Best Interests Determination.
Family Reunion (within programme)	P–3 family reunification program relaunched Oct 2012, DNA evidence of parent-child relationships required, costs reimbursed if relationship proven. Following to join (visa 93) beneficiaries are also counted against the refugee ceilings.

1. RESETTLEMENT POLICY

The United States has a long tradition of granting refuge to those fleeing persecution. Since the Second World War, more refugees have found permanent homes in the United States than in any other country. Admissions of refugees of special humanitarian concern to the United States, as well as admission of those for the purpose of family reunification are important tenets of the U.S. refugee resettlement programme.

At the Federal level, the Bureau of Population, Refugees, and Migration (PRM) of the Department of State administers the U.S. Refugee Admissions Programme in conjunction with U.S. Citizenship and Immigration Services (USCIS) of the Department of Homeland Security and the Office of Refugee Resettlement (ORR) of the Department of Health and Human Services (HHS). Non-governmental organizations play a major role in domestic resettlement activities and, along with the International Organization for Migration (IOM), in overseas processing.

2. CRITERIA FOR RECOGNITION OF REFUGEE STATUS ELIGIBILITY AND ASYLUM

A person must meet the U.S. definition of a refugee found in Section 101(a)(42) of the Immigration and Nationality Act (INA), which closely follows the definition in the 1951 UN Convention. The INA also defines as refugees, under certain circumstances specified by the President, certain persons who are within their country of nationality, or if they do not have a nationality, the country in which they are habitually residing (See Annex B).

3. CRITERIA FOR RESETTLEMENT

To qualify for refugee resettlement to the United States, refugees must:

(1) Be among those refugees determined by the President to be of special humanitarian concern to the United States;

(2) Meet the definition of a refugee pursuant to Section 101(a)(42) of the INA (see below);

(3) Not be firmly resettled in any third country; and

(4) Be otherwise admissible under U.S. law.

Section 101(a)(42) of the Immigration and Nationality Act (INA)

The term "refugee" means:

(A) Any person who is outside any country of such person's nationality or, in the case of a person having no nationality, is outside any country in which such person last habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion, or

(B) in such circumstances as the President after appropriate consultation (as defined in Section 207(e) of this Act) may specify, any person who is within the country of such person's nationality or, in the case of a person having no nationality, within the country in which such person is habitually residing, and who is persecuted or who has a well-founded fear of persecution on account of race,

religion, nationality, membership in a particular social group, or political opinion.

The term "refugee" does not include any person who ordered, incited, assisted, or otherwise participated in the persecution of any person on account of race, religion, nationality, membership in a particular social group, or political opinion.

For purposes of determinations under this Act, a person who has been forced to abort a pregnancy or to undergo involuntary sterilization, or who has been persecuted for failure or refusal to undergo such a procedure or for other resistance to a coercive population control programme, shall be deemed to have been persecuted on account of political opinion, and a person who has a well-founded fear that he or she will be forced to undergo such a procedure or subject to persecution for such failure, refusal, or resistance shall be deemed to have a well-founded fear of persecution on account of political opinion.

4. RESETTLEMENT ALLOCATIONS/PROCESSING PRIORITIES

The administration annually consults with the Congress on the U.S. refugee admissions programme. These consultations provide an opportunity for Congress and Administration representatives: the Department of State, the Department of Homeland Security, and the Department of Health and Human Services; to discuss the international and domestic implications of U.S. refugee policy. These consultations are the culmination of a many-faceted, consultative process that includes discussions with Congressional staff, representatives of State and local governments, public interest groups, international and non-governmental organizations such as the Refugee Council USA (RCUSA) and others concerned with refugees. During the Congressional consultations, the President's proposed refugee admissions programme for the coming fiscal year is presented. This proposal includes information on refugee admissions levels, groups of refugees of special humanitarian interest to the United States, and processing priorities.

The processing priorities serve as guidelines to determine eligibility for access to the U.S. Government (USG) resettlement programme and as a tool to manage the refugee admissions process within the established annual regional ceiling.

The following priorities are in effect for Fiscal Year 2015 (1 October 2014–30 September 2015):

Priority One

UNHCR, U.S. Embassy, or specially-trained non-governmental organization identified cases: persons facing compelling security concerns in countries of first asylum; persons in need of legal protection because of the danger of refoulement; those in danger due to threats of armed attack in an area where they are located; or persons who have experienced recent persecution because of their political, religious, or human rights activities (prisoners of conscience); women-at-risk; victims of torture or violence, physically or mentally disabled persons; persons in urgent need of medical treatment not available in the first asylum country; and persons for whom other durable solutions are not feasible and whose status in the place of asylum does not present a satisfactory long-term solution. As with all other priorities, Priority One referrals must still establish past persecution or a credible fear of future persecution from the country from which they fled. All nationalities are eligible for processing under Priority One.

Priority Two (P–2)

Specific groups of special concern (within certain nationalities) as identified by the Department of State in consultation with NGOs, UNHCR, DHS, and other area experts as well as some in-country programs. Only those members of the specifically identified groups are eligible for Priority Two processing. Each group will be selected based on its individual circumstances.

In-country Priority Two programs include:

Former Soviet Union

This Priority Two designation applies to Jews, Evangelical Christians, and Ukrainian Catholic and Orthodox religious activists identified in the Lautenberg Amendment, Public Law No. 101–167, § 599D, 103 Stat. 1261 (1989), as amended ("Lautenberg Amendment"), with close family in the United States.

Cuba

Included in this Priority 2 program are human rights activists, members of persecuted religious minorities, former political prisoners, forced-labor conscripts (1965–68), persons deprived of their professional credentials or subjected to other disproportionately harsh or discriminatory treatment resulting from their

perceived or actual political or religious beliefs or activities, and persons who have experienced or fear harm because of their relationship—family or social—to someone who falls under one of the preceding categories.

Iraqis Associated With the United States

Under various Priority 2 designations, including those set forth in the Refugee Crisis in Iraq Act, employees of the U.S. Government, a U.S. Government-funded contractor or grantee, and U.S. media and NGOs working in Iraq, and certain family members of such employees, as well as beneficiaries of approved I–130 (immigrant visa) petitions, are eligible for refugee processing in Iraq.

Minors in Honduras, El Salvador, and Guatemala

Under this new P–2 program, certain lawfully present qualifying relatives in the United States can request access to a refugee interview for an unmarried child under 21 in his/her country of origin.

Priority Two groups outside the country of origin include:

Ethnic Minorities and Others From Burma in Camps in Thailand

Individuals who have fled Burma and who are registered in nine refugee camps along the Thai/Burma border and who are identified by UNHCR as in need of resettlement are eligible for processing.

Ethnic Minorities From Burma in Malaysia

Ethnic minorities from Burma who are recognized by UNHCR as refugees in Malaysia and identified as being in need of resettlement are eligible for processing.

Bhutanese in Nepal

Bhutanese refugees registered by UNHCR in camps in Nepal and identified as in need of resettlement are eligible for processing.

Iranian Religious Minorities

Iranian members of certain religious minorities are eligible for processing and benefit from a reduced evidentiary standard for establishing a well-founded fear of persecution, pursuant to the 2004 enactment of Pub. L. 108–199.

Iraqis Associated with the United States

Under various Priority 2 designations, including those set forth in the Refugee Crisis in Iraq Act, employees of the U.S. Government, a U.S. Government-funded contractor or grantee, and U.S. media and NGOs working in Iraq, and certain family members of such employees, as well as beneficiaries of approved I–130 (immigrant visa) petitions, are eligible for refugee processing.

Congolese in Rwanda

Certain Congolese who verifiably resided in Mudende Camp, Rwanda during one or both of the massacres that took place in August and December of 1997 are eligible for processing.

Priority Three

Nationals of the following countries who are spouses, unmarried sons and daughters under 21 years of age, and parents of persons admitted to the United States as refugees or granted asylum, or persons who are lawful permanent residents or U.S. citizens and were initially admitted to the United States as refugees or granted asylum:

- Afghanistan
- Bhutan
- Burma
- Burundi
- Central African Republic
- Chad
- Colombia
- Cuba
- Democratic People's Republic of Korea (DPRK)
- Democratic Republic of Congo (DRC)
- El Salvador
- Eritrea
- Ethiopia
- Guatemala
- Haiti
- Honduras

- Iran
- Iraq
- Mali
- Somalia
- South Sudan
- Sri Lanka
- Sudan
- Syria
- Uzbekistan

Admissibility for Resettlement

Section 212(a) of the INA lists grounds under which aliens may be excluded from the United States.

Refugees may be excluded for the following reasons:

(1) Health-related.—Some communicable diseases, physical or mental disorders, and current drug abuse or addiction (Health-related denials may be overcome when the problem has been successfully treated, or upon waiver at the discretion of the Secretary of Homeland Security).

(2) Criminal activity.—Individuals, who have committed crimes of moral turpitude, drug trafficking, multiple criminal convictions, prostitution, aggravated felonies or acts involving persecution or torture.

(3) Security grounds.—Espionage, terrorist activity, membership in Communist or other totalitarian parties, Nazi persecution or genocide, or individuals who would present a serious security threat. Refugee applicants must clear a series of biographic and biometric checks prior to final approval.

Waivers of certain grounds of inadmissibility may be available in some cases for humanitarian purposes, to assure family unity, or when it is otherwise in the public interest. Requests for waivers for refugees (Form I–602) should be sent to the Field Office Director of the overseas DHS Office with jurisdiction over the case. DHS has sole authority to determine whether or not to waive these ineligibilities for refugees.

5. SUBMISSION AND PROCESSING VIA DOSSIER SELECTION

The U.S. refugee resettlement programme does not admit refugees by dossier selection. All refugee applicants must be interviewed by a DHS officer.

6. SUBMISSIONS AND PROCESSING VIA IN-COUNTRY SELECTION

With respect to a person applying in a third country for admission to the United States as a refugee, an initial review is undertaken to evaluate cases based on the applicants' situation in temporary asylum, the conditions from which they have fled, U.S. National interest, and other humanitarian considerations. Applicants who claim persecution or a well-founded fear of persecution and who fall within the priorities established for the relevant nationality or region are presented to DHS for determination of eligibility for admission as a refugee under Section 101(a)(42) of the INA.

6.1 Case Documentation

Applicants may submit a variety of documentation to corroborate their claims, such as country conditions reports; death certificates; baptismal certificates; prison records; arrest warrants; affidavits of or letters from government officials, friends or family members, and union, political party, or organization membership cards. Refugees are often unable to provide documentary evidence, however, due to the circumstances that give rise to flight. In such cases, testimony, if credible, may be enough to establish eligibility for refugee status without corroborating evidence. If documents are presented, they are reviewed by the interviewing officer for content and authenticity.

6.2 Routing of Submissions

All refugee applicants must ultimately be interviewed by a DHS Officer. USG-funded Resettlement Support Centers (RSCs), previously known as Overseas Processing Entities (OPEs), usually managed by resettlement agencies or IOM, prepare cases and schedule interviews within their regions.

Some processing locations have DHS officers permanently assigned who may adjudicate refugee applications (e.g. Rome, Nairobi, Accra, Vienna, Moscow, Athens, Bangkok, New Delhi, Havana, and Mexico City, among other locations).

In locations that do not have a regular DHS presence, the USG and the RSC work together to schedule visits from DHS officers on a circuit ride basis. The vast majority of refugee adjudications are conducted by DHS officers on circuit ride, and the U.S. refugee admissions programme is committed to frequent circuit rides to posts

where there are sufficient numbers of UNHCR- and Embassy-referred cases or others who are eligible.

For those cases approved by DHS, the RSCs make preparation for onward movement to the United States by arranging medical examinations and a resettlement agency sponsor. IOM makes travel arrangements once the final clearances have been obtained.

6.3 Decision-Making Process

Section 207 of the INA grants the Secretary of Homeland Security the authority to admit, at his/her discretion, any refugee who is not firmly resettled in a third country, who is determined to be of special humanitarian concern, and who is admissible to the United States.

The authority to determine eligibility for refugee status has been delegated to DHS/USCIS. USCIS officers conduct non-adversarial, face-to-face interviews of each applicant to elicit information about the applicant's claim for refugee status and any grounds of ineligibility. U.S. Customs and Border Protection (CBP) screens arriving refugees for admission at the port of entry.

6.4 Recourse Processing

There is no formal procedure for appealing the denial of refugee status, although an applicant may file a Request for Review (RFR) of his case to DHS on the basis of additional evidence or information not available at the time of the interview.

6.5 Processing Times

The time required to process a refugee claim varies considerably based on such factors as the availability of a DHS officer to adjudicate the claim, RSC processing capabilities, type of security checks required, and whether an applicant is admissible to the United States. A very rough estimate of the time it takes from DHS approval of the refugee application until departure is generally 6 to 12 months. Emergency cases may be expedited and have occasionally been processed in a very short time, depending on the circumstances

7. EMERGENCY CASES/URGENT CASES

U.S. capacity to resettle emergency cases is limited by stringent security clearance procedures, the regulatory requirement for a face-to-face interview with all applicants, and enhanced protocols for detecting and treating tuberculosis overseas. The U.S. does not have a quota for emergency or urgent cases, and does not have a specific processing time frame for such cases, but under limited circumstances can process urgent cases in approximately 16 weeks.

In most cases, the U.S. will encourage UNHCR to transport a case to an Emergency Transit Facility (ETF) for U.S. processing if protection-related concerns require the individual to depart the country of asylum in less than 16 weeks.

8. SPECIAL CATEGORIES/SPECIAL NEEDS

The U.S. does not have sub-quotas dedicated to specific needs cases, and accepts UNHCR referrals of all types of special needs cases without imposing a numerical cap.

9. MEDICAL REQUIREMENTS

The Centers for Disease Control and Prevention (CDC) provides the Department of State with medical screening guidelines for all examining physicians, which outline in detail the scope of the medical examination for U.S.-bound refugees. The purpose of the medical examination is to identify applicants with health-related conditions that render them inadmissible to the United States.

Medical screening is mandatory for all refugees. Medical exams are performed by U.S. Embassy-contracted panel physicians or by IOM. The costs for medical exams are borne by the USG. Costs for medical treatment necessary to make an already approved refugee ready for travel are usually paid by the USG. Medical exams are valid for 3 months, 6 months or 1 year, depending on the location and the TB classification, and must be valid at the time of departure for the United States. Screening is generally coordinated by the RSC.

A refugee who is determined (in accordance with regulations prescribed by the Secretary of Health and Human Services) to have a communicable disease of public health significance; a physical or mental disorder and behavior associated with the disorder that may pose, or has posed, a threat to the property, safety, or welfare of the alien or others; or is determined to be a drug abuser or addict, is excludable.

As of January 4, 2010, HIV infection is no longer an excludable condition. A waiver for the above excludabilities is available and must be approved by USCIS.

The U.S. provides pre-departure presumptive treatments in certain locations. In FY 2014, this includes presumptive treatment for malaria and parasites in some locations. Although refugees are not required to receive vaccinations prior to departure, the U.S. administers vaccines in locations where an outbreak of disease, such as measles, occurs in a refugee camp or other location where U.S. refugee processing is taking place. In 2013, the U.S. began routinely administering pre-departure vaccinations in certain locations. As of June 1, this included Thailand and Nepal. The U.S. expanded pre-departure vaccinations to Malaysia, Kenya, and Ethiopia, and Uganda by the end of FY 2014.

10. ORIENTATION (PRE-DEPARTURE)

The Department of State strives to ensure that refugees who are accepted for admission to the United States are prepared for the significant life changes they will experience by providing cultural orientation programs prior to departure for the United States. It is critical that refugees arrive with a realistic view of what their new lives will be like, what services are available to them, and what their responsibilities will be.

Resettlement Support Centers (RSCs) conduct one-to-five-day pre-departure cultural orientation classes for eligible refugees at sites throughout the world. In an effort to further bridge the information gap, for certain groups, brief video presentations featuring the experience of recently resettled refugees of the same ethnic group are made available to refugee applicants overseas.

Prior to arrival in the United States, every refugee family receives Welcome to the United States, a resettlement guidebook developed with contributions from refugee resettlement workers, resettled refugees, and state government officials. Welcome to the United States is printed in 17 languages: Albanian, Amharic, Arabic, Bosnian/Croatian/Serbian, English, Farsi, French, Karen, Karenni, Kirundi, Kiswahili, Nepali, Russian, Somali, Spanish, Tigrinya, and Vietnamese. The guidebook gives refugees accurate information about the initial resettlement process. The Welcome to the United States refugee orientation video is available in 17 languages: Af-Maay, Arabic, Bosnian/Croatian/Serbian, English, Farsi, French, Hmong, Karen, Karenni, Kirundi, Kiswahili, Nepali, Russian, Somali, Spanish, Tigrinya, and Vietnamese. The Welcome to the United States guidebook was revised in 2013. The new version is more comprehensive and interactive, with student exercises included throughout the workbook.

11. TRAVEL

Refugees approved by DHS generally enter the United States within six to twelve months of approval. Travel is coordinated by IOM, which generally provides interest-free loans for the cost of their transportation to the United States. (A refugee is expected to begin incremental repayment of this loan six months after arrival in the United States, and the total amount is generally expected to be repaid within 3½ years.) Refugees generally travel coach class and must pay for excess luggage. Refugees carry travel papers prepared by the RSC which they must present to DHS officials at the port of entry to the United States.

12. STATUS ON ARRIVAL AND THE PATH TO CITIZENSHIP

At the U.S. port of entry, refugees are admitted to the United States by DHS officials and authorized employment. After one year, a refugee must file for adjustment of status to lawful permanent resident. Five years after admission, a refugee is eligible to apply for U.S. citizenship. Refugees who wish to travel abroad before adjusting to Lawful Permanent Resident Status must first obtain advance permission to re-enter the United States from DHS in the form of a Refugee Travel Document. Voluntary return to the country of persecution or availing oneself of services of that country's Government (e.g. passports) may affect the individual's refugee status. The USG does not impede voluntary repatriation, but USG funding is not generally available for refugees wanting to repatriate. Private organizations and UNHCR may be able to assist refugees who choose to repatriate.

13. DOMESTIC SETTLEMENT AND COMMUNITY SERVICES

13.1 Overview of Services (providers and length of eligibility)

The U.S. resettlement program recognizes the desirability for public and private non-profit organizations to provide sponsorship, reception, and placement services appropriate to refugees' personal circumstances, and to assist refugees to achieve

economic selfsufficiency as quickly as possible. Sponsoring agencies are required to ensure that refugees' basic needs are met: initial housing, essential furnishings and supplies, food or a food allowance, and necessary clothing for a minimum of 30 days after arrival in the United States. Further, sponsoring agencies also provide assistance to access benefits and services, assistance with enrollment in English language training, transportation to job interviews and job training, and orientation about services available in the community and life in the U.S. (employment opportunities, vocational training, education, language classes, personal budgeting, safety, legal requirements, and health care) for a period of no less than 30 days that may be extended up to 90 days after arrival.

Initial reception and placement of refugees is carried out by sponsoring agencies through cooperative agreements with the Department of State. Longer term resettlement resources are provided primarily through assistance programs funded by the Office of Refugee Resettlement (ORR) in the Administration of Children and Families, Department of Health and Human Services. ORR supports domestic resettlement through funds to states, voluntary agencies and community-based organizations to provide for cash and medical assistance, employment and social services. The primary ORR grantees may sub-grant local non-profit organizations, county, and local governments. Private organizations and individuals, such as relatives or friends of the refugee or concerned citizens, may also assist with the refugee's resettlement.

13.2 Reception

An IOM representative meets the refugee at his/her port of entry and when necessary, ensures he/she makes his/her onward travel connections. Sponsoring agencies meet the refugees at their final U.S. destination and transport them to their initial housing, which includes furnishings and supplies, food, clothing. The sponsoring agencies provide basic services for a period of no less than 30 days that may be extended up to 90 days.

13.3 Orientation

The U.S. resettlement program strives to ensure that refugees who are admitted to the United States are prepared for the significant changes they will experience during resettlement. Pre-departure cultural orientation programs are available for refugees at many sites around the world.

After arrival in the United States, the sponsoring agency provides refugees with community orientation, which includes information about the role of the sponsoring agency and those assisting the refugee, public services and facilities, personal and public safety, public transportation, standards of personal hygiene, the importance of learning English, other services available, personal finance, and information about legal status, citizenship, travel loan repayment, selective service, and family reunification procedures.

Refugees may also receive materials in their native language which provide information about life in the United States to ease the transition to a new society and culture. ORR provides technical assistance in domestic cultural orientation to promote and enhance community orientation and supports English language training by funding ESL programs and/or referral activities.

13.4 Housing

Under the guidelines established for reception and placement services by the Department of State, the resettlement agencies ensure that decent, safe and sanitary accommodation, according to U.S. Federal housing quality standards, is made available to the refugee upon arrival.

Refugees reuniting with family may spend some time at their relative's accommodation. ORR provides cash assistance to eligible refugees to cover basic needs such as food, clothing, and housing up to eight months. Within the current code of Federal Regulations, ORR extends social services funding to cover housing expenses.

13.5 Health

Resettlement agencies refer refugees to local health services for a comprehensive health assessment upon arrival in order to identify and treat health problems which might impede employment and effective resettlement. This assessment is provided free of charge. Refugees are eligible to apply for Medicaid or Refugee Medical Assistance (RMA) provided by ORR to cover basic health care costs. ORR ensures medical screening for all refugees through RRMA or Medicaid. ORR covers health and mental health needs of eligible refugees up to eight months through the RMA program. RMA provides medical services to those refugees ineligible for Medicaid.

13.6 Language Training

English language ability is critical to a refugee's successful transition in American society. English as a Second Language (ESL) training programs vary among communities. The local resettlement agency is the best source of information about the availability of such programs. ORR funds a technical assistance provider to promote and support English language training.

13.7 Education

Public schools in the United States are operated by local governments so curriculum and facilities vary. Public school education is free for grades Kindergarten to 12 (approximately ages 5 to 18) and is mandatory for children ages 6 to 16. The resettlement agency will be able to provide more information about school registration and other educational resources in the community. ORR supports the integration of refugee children into the American school system through a refugee school impact grant to refugee-impacted areas.

13.8 Vocational Training

Refugees should be aware that job mobility in the United States is great and that refugees frequently change jobs as technical skills and English ability improve. Refugees should also be aware that foreign job certification is often not valid in the United States and that further training, testing, and/or certification may be necessary for some jobs. Vocational and technical schools train people for special skilled occupations, such as auto mechanics, computer programming, and medical and dental assistants. These programs require varying levels of English language ability and often require payment. The local resettlement agency will be able to provide more information about the availability and cost of such programs.

13.9 Employment-related Training

ORR employability training services are designed to enable refugees to achieve economic self-sufficiency as soon as possible. Employment-related training can include: the development of a self-sufficiency plan, job orientation, job development, job referral, placement, follow-up, English language training, and employability assessment services to include aptitude and skills testing. In addition, services can include career laddering and recertification activities for refugee professionals seeking to fulfill their full career potential.

13.10 Employment

Achieving economic self-sufficiency is the cornerstone of the U.S. resettlement program and getting a job is the first step toward that goal. Many jobs available to newly-arrived refugees are entry-level and refugees are encouraged to improve their language and job skills in order to move up the economic ladder. Refugees receive assistance from the resettlement agency or other employment service program in their community in finding a job, though it may not be in the same field in which the refugee was previously employed. Refugees must have documentation authorizing employment, such as the I–94 form, which they receive from DHS upon arrival, or an Employment Authorization Document (EAD), which they receive from DHS 30 days or more after arrival. The Matching Grant program funded by ORR is particularly focused on intensive case management employability services in support of early self-sufficiency. ORR also provides technical assistance to expand and promote employment opportunities.

13.11 Financial Assistance

The U.S. resettlement program is a public-private partnership. The Department of State provides the sponsorship agency $1,925 per refugee to provide for their basic needs and core services. Of the $1,925 per capita funding, $1,125 must be spent directly on refugees. While affiliates must spend at least $925 on each refugee, they may choose to allocate up to $200 of the $1,125 on other more vulnerable refugees. Federal funding is only intended to provide a portion of the resources needed to serve the refugee. Each sponsoring agency and its affiliates raise private resources, both cash and in-kind, to further address the individual needs of each refugee.

The Department of Health and Human Services is the primary funding source in providing financial assistance to States, counties, and local non-profits to assist refugees become economically self-sufficient as quickly as possible. States, counties, nonprofits, and communities provide additional resources to support such programs. Refugees are eligible to apply for public benefits, cash or food assistance, to cover a portion of their expenses. The level of benefits varies State by State.

13.12 Supplemental Support for Refugee with Special Needs

The Department of State refugee per capita funding provides $200 that a local sponsoring agency can utilize for individual refugees with special needs. Additionally, each community in which refugees are resettled is unique, with different strengths and weaknesses. Recognizing this, each sponsoring agency and its affiliates work to determine the most appropriate placement for each refugee, so that that location best matches the individualized needs of that refugee. Once a placement is determined the local affiliate works with other community partners to prepare for the special needs of the refugee. The Department of Health and Human Services programs and discretionary funding allow for the creation of programs to address the diverse needs of refugees and the communities.

13.13 Mechanism for sharing information with service providers; including details on expected populations, specific cases, and integration issues

The Department of State shares information about expected populations for resettlement with other Federal partners, the sponsoring agencies, and States on an annual and quarterly basis. They in turn provide this information to other service providers. Background information and cultural information is published on certain refugee populations planned for resettlement, which include integration issues. Specific case information is provided to service providers through the Department of State comprehensive database. This gives individual biographic data on each refugee to the sponsoring agency that will resettle the refugee and may be shared with other service providers who will serve that specific case. Pipeline information is available to sponsoring agencies, States, and Federal partners. Individual medical data is provided to the Department of Health and Human Services upon arrival of each refugee to ensure appropriate follow-up. Sponsoring agencies, through this database, then provide a status report on each individual refugee at the end of their reception and placement period.

14. FAMILY REUNIFICATION OF REFUGEES

Family unity is an important element of the U.S. refugee admissions programme. This is reflected in the processing priorities discussed in Section 4, as well as in other refugee and immigrant admissions programmes detailed below.

14.1 National Definition of Family

For U.S. immigration purposes, the validity of a marriage is generally determined by the law in the place of celebration.

There are certain exceptions to that rule. For example, refugees may be prevented from complying with formal marriage registration requirements based on circumstances resulting from their flight from persecution. If a marriage is invalid based on a failure to comply with formal registration requirements, a marriage may still be valid for U.S. immigration purposes if the parties were prevented from formal perfection of the marriage due to circumstances relating to their flight from persecution. Examples of circumstances beyond a couple's control and relating to the flight from persecution would include inability to access host country institutions due to refugee camp policies or conditions, discriminatory government policies or practices, and other consequences of the flight from persecution. A couple who has been prevented from formal perfection of the marriage must also show other indicia of a valid marriage. The relevant considerations may include: holding themselves out to be spouses, cohabitation over a period of time, children born to the union, and the performance of a marriage ceremony.

Common law marriages may be accepted for U.S. immigration purposes if the law of the place of celebration allows a couple to marry by agreement, without formal ceremony, licensing, or registration requirements, and recognizes the relationship as a legally valid marriage. However, common law marriages that are not legal in the place of celebration and are simply de facto cohabitation would not be considered a marriage for immigration purposes under U.S. law.

In July 2013, the Board of Immigration Appeals (BIA) issued a precedent decision in Matter of Zeleniak, 26 I&N Dec. 158 (BIA 2013), recognizing lawful same-sex marriages and spouses if the marriage is valid under the laws of the State where it was celebrated. A same-sex spouse may now be included on refugee application if the applicant and spouse are legally married.

USCIS generally looks to the law of the place where the marriage took place when determining whether it is valid for immigration law purposes. USCIS does not recognize a marriage legally transacted in a foreign jurisdiction if the marriage is contrary to Federal public policy. This includes polygamous marriages and some minor marriages.

According to the U.S. Immigration and Nationality Act (INA) Section 101(a)(35): The term [terms] "spouse," "wife," or "husband" do not include a spouse, wife or husband by reason of any marriage ceremony where the contracting parties thereto are not physically present in the presence of each other, unless the marriage shall have been consummated.

According to INA Section 101(b)(1)(A)-(E): (1) The term "child" means an unmarried person under twenty-one years of age who is:

(A) a child born in wedlock;

(B) a stepchild, whether or not born out of wedlock, provided the child had not reached the age of eighteen years at the time the marriage creating the status of stepchild occurred;

(C) a child legitimated under the law of the child's residence or domicile, or under the law of the father's residence or domicile, whether in or outside the United States, if such legitimation takes place before the child reaches the age of eighteen years and the child is in the legal custody of the legitimating parent or parents at the time of such legitimation;

(D) a child born out of wedlock, by, through whom, or on whose behalf a status, privilege, or benefit is sought by virtue of the relationship of the child to its natural mother or to its natural father if the father has or had a bona fide parent-child relationship with the person;

(E)(i) a child adopted while under the age of sixteen years if the child has been in the legal custody of, and has resided with, the adopting parent or parents for at least two years or if the child has been battered or subject to extreme cruelty by the adopting parent or by a family member of the adopting parent residing in the same household: Provided, that no natural parent of any such adopted child shall thereafter, by virtue of such parentage, be accorded any right, privilege, or status under this Act; or

(ii) subject to the same proviso as in clause (i), a child who:

(I) is a natural sibling of a child described in clause (i) or subparagraph (F)(i);

(II) was adopted by the adoptive parent or parents of the sibling described in such clause or subparagraph; and

(III) is otherwise described in clause (i), except that the child was adopted while under the age of 18 years;

Certain family members may join relatives in the United States by one of the following means:

- A UNHCR referral for the purpose of family reunification (Such referrals follow the procedures outlined in Section 6).
- *An Affidavit of Relationship (AOR)*.—An AOR is a form filed with a resettlement agency by refugees, permanent residents, or American citizens to establish a relationship in order to qualify for consideration under the priority three, family reunification category.
- *Visa 93*.—A resettlement authorization for the spouse and unmarried children under 21 of a refugee already resident in the United States.
- *Visa 92*.—A resettlement authorization for the spouse and unmarried children under 21 of an asylee already resident in the United States.
- *Regular immigration*.—Refugees may also qualify for admission under regular immigration categories if they have the requisite relatives in the United States.

14.2 Family Reunification Eligibility

Use of an AOR requires that the relative applying for U.S. resettlement establish refugee status in his own right and be otherwise admissible for entry into the United States, as determined by DHS. An acceptable AOR permits an applicant to be considered under Priority 3. A Visa 93 or Visa 92 petitioner must establish proof of relationship (spouse or unmarried child under 21). While immediate family members do not need to qualify as refugees in their own right in order to be eligible for Visas 92 or 93 and may still be situated in their countries of origin, they must demonstrate that they meet the required standards regarding admissibility to the U.S.

14.3 Allocations for Family Reunification

All family reunification cases, whether direct applicants, UNHCR referrals or Visas 93 beneficiaries, count against the annual regional refugee admissions ceiling. Visas 92 beneficiaries do not count against the annual admissions ceiling.

14.4 Routing of Applications

UNHCR referrals for the purpose of family reunification follow the procedures outlined in Section 6.

- *AOR*.—A relative in the United States files an AOR with a local branch of one of eleven resettlement agencies with a cooperative agreement with the Depart-

ment of State. If determined to be eligible, routing then follows the procedures outlined in Section 6.

- *Visa 93*.—A refugee in the United States must file Form I–730 (Refugee/Asylee Relative Petition) with DHS on behalf of his/her spouse and minor, unmarried children, along with supporting documentation to verify the relationship. The I–730 must be filed within two years of the refugee's arrival in the U.S.
- *Visa 92*.—An asylee in the United States must also file Form I–730 (Refugee/Asylee Relative Petition) with DHS on behalf of his/her spouse and minor, unmarried children, along with supporting documentation to verify the relationship.

14.5 Case Documentation

When the refugee applicant seeks resettlement in the United States through UNHCR based on family ties, such ties may be supported by a marriage and/or birth certificates, certificates of adoption or approved Form I–130s (Petition for Alien Relative). If these documents are unavailable, a church record, school record or census record showing date and place of birth may be acceptable. If the above documentation is unavailable, the applicant may present a notarized voluntary agency Affidavit of Relationship (AOR), sworn statements of persons who are not related to the principal applicant attesting to the relationship claimed, or, if necessary, such affidavits from persons related to the principal applicant. UNHCR need not request that an AOR be filled out when referring a case under Priority One.

14.6 Processing Times

The processing timeline for family reunification cases is longer than that for UNHCR-referred cases, as the AOR must be vetted by USCIS prior to commencing RSC prescreening, and DNA evidence of certain parent-child relationships, at the applicant's expense, is required. Following a four-year suspension due to relationship/identity fraud, the U.S. re-started the P–3 program on October 15, 2012.

15. REFERENCES/RESOURCES

The following materials are available from any U.S. Embassy that processes refugees or from the Bureau of Population, Refugees, and Migration at the U.S. Department of State:

Center for Applied Linguistics (CAL), *Welcome to the United States: A Guidebook for Refugees.* 2012. *http://www.culturalorientation.net*

Committee on the Judiciary of the House of Representatives. *Immigration and Nationality Act,* May 1995. *http://www.uscis.gov*

U.S. Department of State, Department of Homeland Security, Department of Health and Human Services. *Report to the Congress: Proposed Refugee Admissions for Fiscal Year 2015, September 2014. http://www.state.gov/documents/organization/232029.pdf*

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

Chairman MCCAUL. The Chair recognizes Mr. Katko.

Mr. KATKO. Mr. Chairman, I don't have any reports to put into the record, but I do have a report I want to talk about for a moment.

Chairman MCCAUL. You may.

Mr. KATKO. That is the—I was chair of the joint terrorism task force—the report, *Combating Terrorism and Foreign Fighter Travel.* I appreciate your comments. I am proud of the work that our task force did. Many of my colleagues sitting here today were part of that task force. It was done in a bipartisan manner.

When we did this over a 6-month period of time, we spent an extensive amount of time with folks from Homeland Security, as well as FBI, and spent a lot of time with the National Counterterrorism Center, as well, and we learned an awful lot.

I could be here all day asking you specifics about the report, but I just—a couple things I do want to touch on.

In the wake of 9/11 and the 9/11 Commission, there was legislation passed in 2006 to develop a National strategy to combat for-

eign fighter travel. The landscape has changed tremendously since then, as we all know, especially with respect to ISIS.

One of the report's recommendations is to basically have an updated report of that, and I wanted to hear what your thoughts are on that, all of you.

Secretary JOHNSON. Congressman, in general, I do believe that we need a comprehensive strategy to foreign terrorist fighter travel.

I also agree that since 2006 the threat has evolved enormously, particularly from European countries. We are concerned about those who have been to Syria and who come to this country from a country for which we do not require a visa, which is why, as you know, I announced a number of security enhancements with respect to travel from European countries to deal with this exact threat.

But it is a significant problem, and I agree that we should have—we do have this in very large measure, but we should have a comprehensive overall strategy for dealing with it. We are doing a lot on my end. The FBI is doing a lot on their end to interdict those who are leaving this country who are going to Syria. But this something that is going to be with us for a while. It also involves working with our friends and allies internationally, working with the Government of Turkey, for example, which is something I am personally focused on at the moment.

The last thing I will say, I read most of your report. I didn't get through all of it. I thought it was an excellent report. I complimented one of your staff on the elevator ride up here. I said, "You wrote a great report"——

Mr. KATKO. That made his day, by the way, just so you know. That made his day, that complimenting the staffer. He appreciates that, so thank you.

Secretary JOHNSON. Well, he pointed out to me, "It wasn't me. It was the Members of Congress."

Mr. KATKO. I appreciate that.

Secretary JOHNSON. I thought you would.

Mr. RASMUSSEN. Can I just add on to that, sir?

The one thing we can be sure of is that today's conflict zone is obviously Iraq and Syria, where we are so heavily focused on foreign terrorist fighters, but we can be certain that there is likely around the corner in future years another conflict zone where foreign terrorist fighters will be a problem that we will confront as a matter of National security.

So I think some of the very things your report highlighted—the structures and procedures and capabilities we are putting in place to deal with this problem—don't necessarily give us immediate relief. They don't help us next month tell you that the flow of foreign fighters has been squashed or shut down, but I would argue, importantly, that we are building some capability that will bear out over time.

Similarly, like Secretary Johnson said, so much of the work on this problem is international work right now. I would say that there is a good-news story embedded in this problem in that our foreign partners are far more willing to share information on this problem than would have been the case in 2006 or 2007, when we

were dealing with the foreign terrorist fighter problem at that time.

So, again, the size of the problem, undoubtedly larger and more complex, but the array of resources we are able to call on around the globe, countries with whom you would never think we would be working, we are exchanging successfully information on foreign terrorist fighters.

Mr. KATKO. Right. It seems like the phenomenon with respect to ISIS, at least, and the radicalization of home-grown terrorists here and getting them to go overseas to fight for them is an added twist. So I think that is something that probably warrants an update in the whole terror travel analysis.

Mr. Comey, I know you didn't have a chance to answer, but I do have a question for you that is different in nature, given the short period of time I have. I am concerned about the Joint Terrorism Task Forces, JTTFs, and the stresses that are being put on them.

You traditionally have investigated international and domestic terrorism as part of the JTTF. So, to address a question that was brought earlier, the JTTF doesn't discriminate under which cases they look at. Whatever comes across their radar, whether it is a domestic case or an international case, gets a high priority. Is that correct?

Mr. COMEY. That is correct.

Mr. KATKO. My concern is, grafted on top of that now is this whole new phenomenon about ISIS and the stress that that is putting on, both from foreign fighters coming back, having to expend all the capital and resources to track them, which is very difficult, as well as trying to find a needle in the haystack for those who are getting radicalized over the internet.

So I know you talked about it, but I want to make sure we get a good understanding. Are the JTTFs being stressed beyond the breaking point? Or are they okay? Or do they need more help?

Mr. COMEY. They are being stressed tremendously. As I said earlier, they were very, very stressed in May and June and early July, in particular. But, given your career experience, you know the kind of folks they are. They will just get the work done.

What I want to make sure I do is, if we have a new normal, that we get them the plus-up and resources they may need. I am not in a position yet where I am going to come back and ask for that, but it is something we watch very carefully.

Mr. KATKO. Okay. I understand that working together with the State and local authorities is helping you to leverage that. I encourage what we can to keep that going, because that is a really important aspect of the puzzle. So thank you very much.

I yield back my time.

Chairman MCCAUL. The Chair recognizes Mrs. Torres.

Mrs. TORRES. Thank you, Mr. Chairman.

To FBI Director Comey, I want to thank you personally for the outreach that your L.A. office has done in my district. It was really important for me to ensure that we have a face behind that, you know, phone number that we are supposed to be reporting issues of concern to. They have offered to do a follow-up in a more, you know, law-enforcement-to-law-enforcement, because we did have

members of the community at that hearing. So thank you for that work.

In your testimony, we were talking about terrorist propaganda and the outreach that these terrorist groups are doing through social media. I am very concerned about their infiltration with our local gangs. We have placed a lot of attention and I congratulate all of you on the work that you are doing internationally.

My concern is the Mexican Mafia. My concern is the white supremacist groups that have targeted African-American communities. I want to ensure and be on record that we are doing everything that we can to also follow up on those issues.

Mr. COMEY. Yes, Congresswoman. Thank you for that. Those are an important part of the FBI's work with our local partners all day, every day, the gangs you mentioned, extremists that you mentioned. The Bureau was given the resources after September 11 to make sure we could be great at both our international terrorism responsibilities and these criminal responsibilities.

Mrs. TORRES. Earlier in your testimony, you said that due to sequestration you have had to move people out of criminal investigations to do surveillance work for these potential terrorist folks that go dark. That is why I bring that out to you.

Mr. COMEY. I echo what my colleague Secretary Johnson said about sequestration. One of the reasons we have had to move those resources is we are trying to hire out of the hole that was left for us 2 years ago. So we hired 2,000 people this last year; we are going to hire close to 3,000 this year. So we are trying to dig out of that hole and get us the people who can fill those slots. If we get hit again, I don't know what we will do.

Mrs. TORRES. When we first met last year, I had asked you specifically about ensuring that you hire people, you know, that look like America and that we are targeting areas where we need certain languages and certain ethnic backgrounds to be represented at the FBI table.

How has your progress been on that?

Mr. COMEY. It is probably too early to tell, but we are devoting a tremendous amount of effort to that, to trying to encourage people from all different backgrounds and walks of life to try and get into the FBI. It is not about lowering the standards. We don't need to lower the standards. We just need people to give us a chance.

The obstacle we face, one of my daughters said to me, "Dad, the problem is you are the man." I said, "Thank you." She said, "I don't mean that as a good thing, Dad. You are 'the man.' Nobody wants to work for 'the man.'" You have to change the way they think about it. So we are working very hard about that, for folks to understand that the Bureau——

Mrs. TORRES. Right.

Mr. COMEY [continuing]. Is great place for people, whether Latino, African-American, Asian, men, or women, to work. It is a work in progress. But I have 8 years left, and so I will——

Mrs. TORRES. Thank you.

Mr. Rasmussen, you talked about a creation of community engagement groups. How do you intend to do that? Who are the community partners that you will be inviting to participate?

Mr. RASMUSSEN. In my written remarks, I highlighted the work we are doing at NCTC alongside Secretary Johnson's team and Director Comey's team. I will tell you, though, in this effort to deal with countering violent extremism here inside the United States, it ends up being a separate and distinct conversation in almost every community. Because in each community in which we are working together, all of us, the community leadership looks different, the problem looks different, the set of actors who may have influence looks different. That is what makes it hard.

I think we are doing very good work in this area, but it has been hard to scale up because there is no National-level solution, no single answer, where you say, if you just touch this in Los Angeles, it works in Dallas or it works in Miami or it works——

Mrs. TORRES. That is why it is so important to engage local law enforcement and to ensure that diversity is at the top of our priority.

Mr. RASMUSSEN. I agree completely.

Again, I wouldn't even suggest that we are bringing a solution to those local communities. In many cases, we are bringing information, which will hopefully empower those communities to actually make the choices and the changes and take the steps necessary to deal with extremism in their midst. That is not a Federal solution.

Mrs. TORRES. Thank you.

I yield back my time.

Chairman MCCAUL. The Chair recognizes Mr. Hurd.

Mr. HURD. Thank you, Mr. Chairman.

Thanks to our distinguished panel for being here today. Also, please tell the men and women that work for you all thank you on behalf of us, as well.

I spent 9 years as an undercover officer in the CIA. I was in the CIA when 9/11 happened. To think that, if you would have asked me then that there wouldn't be a major attack on our homeland for over 14 years, I would have said you all were crazy. But we haven't had one, because the men and women in you all's organizations are all working as if it is September 12 every single day. The operational discipline and tenacity that takes, I recognize that and understand that, and my hats go off to them. It is great representing the 23rd Congressional District of Texas, but it is also great representing those men and women that are doing that.

I represent over 820 miles of the border, so, Secretary Johnson, I am here to report to you that you have some hardworking men and women in Border Patrol and Customs along that border. I had the awesome opportunity to award three of them with the Congressional Medal of Valor. They went above and beyond during a flood. It read like straight out of a movie. So I see what these men and women are doing every day.

One issue that they do have is—and don't need to address it here, but I would like to work with your staffs, and it probably impacts the FBI, as well, Director Comey, and this is the right-sizing of the Federal fleet. I think GSA's requirements don't take into account the unique challenges that law enforcement has to deal with, nor folks on the border. So I look forward to working with whoever

in you all's offices on maybe this issue and looking at solving that problem with the GSA.

Secretary Johnson, I am also interested in learning from your staff on how you all calculate got-aways and that process. That is something I would welcome an analysis of that from the correct folks on your team, if that is okay.

My first question to you, Secretary Johnson, is: The cyber deal with China that was recently announced, have we seen any impact that is having on attacks on our critical infrastructure from the Chinese?

Secretary JOHNSON. I would say it is, at this point, too early to make an informed assessment.

One thing that I will be looking to see is whether in our follow-up engagement, which I hope to have in December, we will see real progress, building on what we have agreed to on paper. So that, to me, will be a first indicator of whether or not the Chinese are taking seriously what they agreed to do when they were here in September.

Mr. HURD. Excellent.

Like you in your opening remarks, I hope the Senate sends us a bill so that we can, you know, reconcile those differences and get something to the President to sign, because cybersecurity is important.

Director Comey, I appreciate your opening remarks and your stressing that the Bureau is not seeking any legislative issues regarding the going-dark phenomenon or encryption. Because there is still a perception out there amongst the private sector and privacy groups that the FBI is still looking for a back door or a front door to encryption. We all know that that is technically not able to do that. If you allow the good guys to have access to the back door, then you are allowing the bad guys to have access to the back door.

My question, though, is: When you have groups like ISIS using social media tools to increase their effort, doesn't that also give us an opportunity to increase our targeting of these groups?

Mr. COMEY. Thank you, Congressman.

First, with respect to your predicate, I honestly don't agree with your framing of it, in terms of the encryption issue. I don't think there is a single "it." It is a very complicated technical landscape. I resist the term "back door." I know it dominates the conversation today, but I don't know what the answer is. I see lots of companies who are able to provide secure services to their customers and they still comply with court orders.

So people tell me it is impossible. I am a little skeptical.

Mr. HURD. So here is my question, though. A lot of folks—I have sat down and talked with these people and talked with people in your organization about, give me the use cases in which the case actually went cold. Because even if you have people using a device, you may not get the plain text information, but you do have the device. You do know that someone is using that. You do know the location of that device.

So saying that you still can't target terrorists that way and throwing certain companies under the bus by saying they are not

cooperating, I don't think that is an accurate portrayal of what is really going on.

Mr. COMEY. Yeah, and I hope you didn't hear me to throw anybody under the bus. We are collecting and we will get you hundreds and hundreds of cases. But, to me, that actually doesn't—I think everybody agrees the logic of encryption means that all of our work will be severely affected by it, but I don't think that is the end of the conversation.

The question is: How much do we care about that, and what can we do about it? We will demonstrate the cases where it affects criminal work and intelligence work and National security work, but I don't think that ends the conversation.

Mr. HURD. I 100 percent agree.

I disagree a little bit with some of your opening remarks that there is a conflict in our values. I don't think there is a conflict of our values. Our civil liberties are the things that make our country great. We can protect our civil liberties and our digital infrastructure and give our men and women that are working hard to keep us safe every single day the tools they need in order to continue to protect us in an increasing environment.

I am over my time. I look forward to working with you on this issue and the private sector, because this is something that we can solve.

I yield back, Chairman.

Chairman MCCAUL. The Chair recognizes our first female combat pilot, Ms. Martha McSally.

Ms. MCSALLY. Thank you, Mr. Chairman.

Thank you, gentlemen, for your testimony and the hard work of you and all the men and women that are in your organizations.

I was on the task force. I was proud to be on the task force. Certainly very eye-opening and troubling, but very important work for us to identify some of the challenges and loopholes we have, which have been, you know, further discussed in your testimony today. Look forward to working with you all to see how we can, you know, obviously, close those loopholes and increase our security.

I want to specifically talk about the recruitment of women and girls. We have talked about, you know, we think there are over 250, maybe, Americans have been recruited, over 2,500 Westerners. A lot of the men are being recruited to go over and join the caliphate to fight, but women and girls are been recruited to go over and basically be subjected to sexual slavery—a very different dynamic. We have heard reports that the women and the girls, quite frankly, can't leave in the same freedom as some of the men do.

So do any of you have comments about the different dynamic there and then different efforts we would have in order to counter the violent extremism and the recruitment of women and girls?

Mr. RASMUSSEN. It is a very good question. What we do know is that ISIL does prioritize trying to recruit and bring young women to the caliphate. They target some of their messaging directly to that community, and they adopt themes that they think will resonate with young women in Western Europe and even here in the United States.

You will probably remember, not too long ago, *The New York Times* ran a very disturbing series on the front page that described

in some very vivid detail some of the horrific experiences young women have been put through by moving to the caliphate.

I was heartened to see that that kind of information was becoming public, because it can only help to have that information exposed. But is *The New York Times* going to be the vehicle that reaches young women and explains to them how at risk they are if they respond to this call or, in the way that Director Comey described in his opening remarks, the way they gravitate, the way they might choose to gravitate towards the positive ends of this message? I don't think *The New York Times* is going to be the vehicle that helps us explain that and create that sense of awareness that it is not the environment they are signing up for.

Ms. MCSALLY. Right.

Secretary JOHNSON. Congresswoman, I think a fundamental part of our CVE efforts here in this country is a message that has to be addressed to young women about the type of exploitation they could be subjected to——

Ms. MCSALLY. Right.

Secretary JOHNSON [continuing]. If they go to these places. But I also believe it includes a message to their parents, as well——

Ms. MCSALLY. I agree. Thank you.

Secretary JOHNSON [continuing]. Their family units.

Ms. MCSALLY. Great. Thanks.

Moving on to a different topic, we have had a lot of discussion today about vetting the refugees. We identified in the task force some challenges with the Visa Waiver program and, you know, just making sure, again, that we are keeping the country safe.

One of the elements—we had a demonstration out of the university in my district, University of Arizona, related to deception-detection technology. What we have learned in some of the briefings I have gotten is, even with a face-to-face interview, you often could be wrong if someone is trying to deceive. There has been decades of work done in identifying through, you know, neurological means and other things whether somebody is deceiving, whether that is filling out on-line forms or in person.

We did give a demo to some individuals in your organization, but I would really like to follow up with that, because I think these are some cheap technologies that we could deploy that helps us in the vetting fight for a variety of different dynamics here. I know some of your members were there, but it is sometimes difficult, you know, bureaucratically, to move technology quickly.

So I would really like to follow up with all of you related to this deception-detection technology, because I think it really would be helpful, if you are open to it.

Secretary JOHNSON. Yes.

Ms. MCSALLY. Great. Thank you.

Then the last thing is, you know, I ran the counterterrorism operations at AFRICOM in my last military assignment. We talk about foreign fighters and foreign fighter training. Working with your organizations, you know, we were watching thousands and thousands of terrorists being trained in al-Shabaab training camps, and we had the authority, but we didn't really have the will to do anything about it.

You know, we are all talking about ISIS right now, but we do have AQIM, AQAP, al-Shabaab, certainly with the challenges with pulling out some forces in Yemen, limiting our intelligence. Just wanted some discussion on that so that we are not all focused on ISIL and not, you know—I know your organizations are not, but I just want to hear your assessments of addressing the AQAP, AQIM, and al-Shabaab threats.

Are there any similar issues that we don't have the will to be addressing those? Or what other challenges are you having with those threats?

Mr. RASMUSSEN. Thank you for raising that issue, because, as you saw in my remarks, I resist a little bit the kind of gravitational pull that says that ISIL is the sole focus of our counterterrorism effort right now. It is certainly—as I said in my testimony, the group has surpassed al-Qaeda in terms of its prominence in leading a global jihadist movement, but, in terms of the threat we face, each of the groups you rattled off, Congresswoman, very, very dangerous, lethal, and deserving of all of the resources and analysis we can bring to bear on it as a counterterrorism community.

Simply as a matter of workforce management, I have had to resist the pull also to, again, surge analysts in the direction of only working on ISIL-related threats because of the array of other places around the world where al-Qaeda, al-Qaeda affiliate groups, and other extremist groups are potentially threatening us. So thank you for raising that.

Ms. MCSALLY. Great. Thanks.

My time has expired, but I look forward to following up with your organizations on those threats, as well.

Thank you.

Chairman MCCAUL. The Chair recognizes Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Mr. Chairman.

Thank all of the witnesses for all that you do to keep America safe.

I would like to go back to the issue in Syria that has displaced millions of folks seeking refugee status around the world. Obviously, it is a humanitarian concern for all of us. I am certainly sympathetic to the atrocities there. Like many of the Members have mentioned, I appreciate our country's profound and long-time commitment to providing a place of security to those fleeing disastrous conflicts.

That being said, I did want to drill down a little bit on the President's announcement a month ago of a 600-percent expansion in the number of Syrian refugees allowed into this country, going from about 1,600 a year to a figure of at least 10,000, as the President mentioned. I think, Secretary, you clarified that number today.

So, while humanitarian concerns are certainly warranted—we know that—I know that you would all agree with me that the President's actions certainly raise some real security risks here at home.

Director Comey, you have recently testified before the Senate that, while we do have a robust screening process here, I think you did acknowledge that at the same time there are some information

gaps in our databases that we use to screen these individuals. Is that correct?

Mr. COMEY. That is correct.

Mr. RATCLIFFE. Okay.

But, again, I know you all agree that it is also vitally important that we understand who is coming into this country to the best of our ability, especially when we also know that ISIS has expressed an interest and an intent in using the refugee process to get in the United States.

That is also a fact, isn't it, Director?

Mr. COMEY. Yes. I think Director Rasmussen testified to that just a few minutes ago.

Mr. RATCLIFFE. All right. So with that in mind, I think we are all agree that it is imperative these decisions be made on an humanitarian basis, but also with respect to National security in mind, and each of you and your respective teams are full of extremely talented, capable, dedicated folks that can inform these decisions, and so I want to find out the extent to which they were utilized.

Was the figure announced by the President of 10,000, was that the product of a thorough analysis by your respective agencies? I will start with you, Secretary.

Secretary JOHNSON. The announcement of 10,000 was the product of considerable interagency discussion. My Department and USCIS was certainly consulted in arriving at that number. It is, as I think you noted very definitely, striking a balance between what we know we can accomplish with the resources we have, and not shutting our eyes and our doors to what is really a horrible world situation and doing our part to try to alleviate it. But yes, we were consulted, sir.

Mr. RATCLIFFE. Great. Thank you.

Director Comey.

Mr. COMEY. That is my understanding as well. There was an interagency process run through the National Security Council, and the FBI was a participant in those conversations.

Mr. RATCLIFFE. Okay. Director Rasmussen.

Mr. RASMUSSEN. The same as well.

Mr. RATCLIFFE. Okay. Thank you.

Director Rasmussen, I want to talk to you a little bit. Back in June, we held a hearing at this committee called "Terrorism Gone Viral," and it really examined the terrorist attack in Garland, Texas, which is just outside of my district, and related to ISIS's use of the social media, which is something that we have all talked about a lot today.

In our June hearing, I really tried to get answers on the issue of why ISIS has been so skillful in this area relative to other foreign terrorist organizations. I asked about whether or not it was due to better funding, or whether it was certain individuals within the group. The responses I got were largely, well, the internet hadn't really developed when al-Qaeda was going; social media wasn't as pervasive until recently. But I think those responses ignored the fact that, you know, at present, other terrorist organizations certainly exist, but it appears that ISIS still remains uniquely skilled in this area.

So you gave some testimony recently in an exchange with Senator Johnson at the Homeland Security Committee in the Senate, and I wanted to ask you a little bit about that. Maybe it relates to—I know there were reports in September that ISIS's social media activities seem to ramp down following the death of Junaid Hussain, but I guess I want to know your opinion. Is ISIS unique in recruiting foreign fighters and inspiring lone-wolf attackers? Is that a product of some unique capability that they have? If not, are there other factors, or what are the other factors that make ISIS so skillful in this area?

Mr. RASMUSSEN. I hesitate to use the word "unique," because, you know, the capabilities that they are using to mobilize potential fighters or terrorists, those aren't necessarily things that can't be transferred or adopted by other groups going forward. I think the innovation that ISIL, as an organization, undertook that differentiated it from al-Qaeda in a significant way was that ISIL truly did aspire to be a mass movement.

In creating the caliphate, the idea was to populate the caliphate with individuals all around the world. Al-Qaeda traditionally and typically operated as a clandestine terrorist movement, where vetting processes and letting individuals into the group was a very serious business. So you did not see al-Qaeda—I would argue they probably didn't have the tools to do this, but they were not seeking to create a mass organization capable of controlling territory the way Iraq—in Iraq and Syria the way ISIL has.

So I would hate to rule out, though—or I would hesitate to rule out that other terrorist organizations could not adopt the same kinds of skillful techniques that ISIL has.

Mr. RATCLIFFE. Thank you.

I yield back.

Chairman MCCAUL. I was just informed that—for the Members, that Director Comey has a hard stop at 12:30. So just take that into consideration.

The Chair recognizes Mr. Donovan.

Mr. DONOVAN. Thank you, Mr. Chairman.

Gentlemen, my colleagues have articulated the incredible responsibility you all have protecting our country from domestic homegrown radicalized individuals to people who are overseas who want to attack our country to fighting mass—possible mass destruction in our country to lone wolves shooting up people who are worshipping in a church in the South. Tremendous. I want to just touch on something that no one has touched on yet, and that is the possibility of nuclear devices.

Director Comey, your agents have done a remarkable job in thwarting smugglers from trying to equip ISIS with nuclear materials. Recently, one was reported, and I think there were 4 others, or 5 others, during the last few years.

Are we getting some assistance from some of the former Soviet countries? Russia also would be threatened by this. What other materials possibly should we be looking towards other than just nuclear devices? Certainly, I know there are other materials that have been harmful to our country, but what other materials that people like these—ISIS or al-Qaeda other groups are looking to use against our country?

Mr. COMEY. Thank you, Congressman. The answer is we get cooperation across the board on this, because whatever people's political difference is, everybody understands the threat posed by radiological nuclear chemical biothreats. So we have invested as a country, and the FBI in particular, in building relationships with our counterparts, you know, a whole host of Eastern European countries, the former Soviet States there, so that is a good news story.

The challenge we all face is, ISIL's mission is simply to kill a lot of people. So they are not in love with any particular tool, as long as it will kill people. So we focus on, obviously, devices themselves, but also radiological materials, that might—a cesium that might be used to terrify people or to injure people, a long-term radiological illness. So there is a broad spectrum there.

As I said earlier, we have folks in the FBI, and I know my partners here do, that wake up every day focused just on this, because we see the threat as low probability, huge impact.

Mr. DONOVAN. Thank you, my fellow New Yorker. My other fellow New Yorker, Secretary Johnson. Yesterday Congress passed a bill of mine to authorize Securing the Cities, a pilot program that your agency started back in 2006, very successful in New York, New Jersey region, expanded to Houston, Los Angeles, Long Beach area, District of Columbia. The efforts that you are making there, because we are expanding, do you have the resources to continue the success of that program in the future, because it has been remarkably successfully in our area, where you and Director Comey and I come from, and the successes that we have heard from my colleagues are just remarkable.

Secretary JOHNSON. My assessment of the Securing the Cities program is that it has been very successful, and it is very important and very valuable. So thank you for your support for it. As you noted, we have moved to other cities, and I think we need more of that. We try to do three or more cities at a time, but—it is a valuable program, and I know that there are more cities out there that can definitely benefit from this.

Mr. DONOVAN. I am sorry, Mr. Rasmussen. If you are not from New York, I am not going to ask you a question.

My time is up. Thank you.

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

Chairman MCCAUL. I thank you for that. The Chair recognizes Mr. Richmond.

Mr. RICHMOND. First of all, let me thank the Chairman and the Ranking Member and thank the witnesses who do a very difficult job and very difficult circumstances with ever-changing technology.

I would hate to be in your job. But let me just ask, and I know there is a lot of talk about a number of issues, but I am going to get a little local in my area, because we do have the largest petrochemical footprint in the United States in my district, and we also have millions and millions of visitors that come, and then we also have the largest port complex in the United States in my district.

So as you all share intelligence, and as you all go about protecting the homeland, how worried are you all about our port security, our chemical facility security, our refinery security, and our ability to protect them?

Secretary JOHNSON. Well, let me begin with that. New Orleans is a confluence of things that we in Homeland Security are concerned about, as you have laid out in your question, Congressman. Given the—and so it is rightly on our radar.

Given the nature of the threat we face, it is difficult to rank with any real degree of certainty where we should focus on and what we should not focus on. For example, I think all of us would agree that prior to this summer, we didn't have any particular reason to put Chattanooga, Tennessee high on anybody's list. So given the—given the range of threats we face, we have to be vigilant in a bunch of different places, but certainly port security, maritime security, and the other things that converge in New Orleans are areas where I know many aspects of our Department are focused in.

Mr. RICHMOND. Mr. Comey.

Mr. COMEY. Congressman, I don't think I have anything to add to what Jeh said. Except, you know, because we have a lot of folks working in your district, it is a big focus of our work. We do face a large array of threats, but we try to focus resources on the big attractants for terrorist activity to try and make it harder for them, and a big piece of that is focusing on ports, on tourist locations, and on travel locations.

Mr. RICHMOND. Let's spend just a quick second talking about the encryption and the back door. I guess my question, and I guess it is a technical question, that if our tech companies create the back door, aren't there apps or over-the-counter things that would also allow people to encrypt it, or are you all pretty confident that you can access data through any over-the-counter encryption?

Mr. COMEY. Thank you for that question. As I said to Congressman Hurd earlier, I resist the term "back door," because mostly I don't understand what it means. What we are looking for is a world in which, ideally, when judges issue court orders to search a device or to intercept communications, companies are able to comply with that. Today, lots of the most sophisticated internet service providers are able to comply. Their systems, no one is telling me, are fatally insecure. Like some of the biggest email providers in the world, based in the United States, comply with our court orders. So I actually don't think the problem is one of technology, I think it is one of business model. There are lots of companies who have said: We will never do this for the Government. So that is a problem we have to figure out how to solve.

But here is the bad news: Commercially-available encryption, strong encryption, we cannot break it. So we find ourselves getting court orders from judges. We make a showing of probable cause, judge gives us permission for a limited period of time to intercept, we can't unencrypt that data, so we are out of luck. So we have to figure out other ways to try and make that gang case, that kidnapping case, or that terrorism case.

Mr. RICHMOND. Thank you. I see my time has expired. I yield back.

Chairman MCCAUL. Mr. Barletta.

Mr. BARLETTA. Thank you, Mr. Chairman.

This morning, *The Daily Caller* reported that the U.S. attorney for the Eastern District of Virginia has indicted two senior NASA managers, NASA managers, at the Langley Research Center for

willfully violating National security regulations while allowing a visiting Chinese foreign national to gain complete and unrestricted access to the Center.

If this wasn't troubling enough, the article reports that in the wake of this case involving alleged espionage by a Chinese national, and now foreigners have more, not less, access to NASA operations at present.

Before the Bo Jiang case, all foreign nationals, including green card holders, could be monitored and restricted. But now green card holders are treated like U.S. citizens with unrestricted access to all parts of the space research facility. It quotes a senior NASA official as saying, "If you have a green card, your allegiance may still be to China, but the green card gets you legal authority to work in the United States; therefore, we don't track them. They don't have any restrictions to transfer technology-controlled plans. They are given access to the same exact way as a U.S. citizen, because they have a green card."

First, I would like to commend Director Comey and the FBI for their role in pursuing this case over the last several years. But, second, I would like to ask the panel whether this is common practice that non-U.S. citizens holding green cards, but with sworn allegiance to other countries, have the same access and privileges as a U.S. citizen at NASA centers and other facilities that may be of interest to foreign intelligent services? If so, why?

Secretary JOHNSON. I am sure that Nick and Jim have their own answers to this. I will just say—I haven't read the particular article, Congressman, that you are referring to. I have been in countless places in Government buildings, sensitive areas, where the sign says, U.S. citizens only, who obviously have their requisite security clearances. I can't tell you the number of places where I see that. It is fairly common. I don't know about the particular circumstance that you are referring to there, but I will be happy to refer to my friends here.

Mr. COMEY. Congressman, obviously, because the case is pending, I am not going to comment on the case. I thank you for the kind words about our folks who worked hard on it. I think the issue that you are talking about with NASA is about access by foreigners to Unclassified information. As Secretary Johnson said, there is a whole regime that is very tight around what access foreigners might get to Classified information. I think the issue there is when green card holders wander around a space that is not Classified, what of America's information can they see there. Honestly, I am not smart enough on the issue right now to talk to you about in this forum, but it is something we have to get smarter about.

Mr. BARLETTA. Sure.

Mr. RASMUSSEN. With respect to my organization, we operate in a highly Classified environment, and any foreign national or non-security clearance holding individual would be required to be strictly escorted around our facility, again, as in any place in the intelligence community.

Mr. BARLETTA. Do you think this committee should look at changing security laws and access by green card holders to bolster defense at these Federal facilities, or are you satisfied with what we have in place?

Mr. COMEY. I will answer with another that I don't know. Again, with respect to access to Unclassified information, I don't know enough about the issue sitting here to offer you a view on it.

Secretary JOHNSON. I would have to give the same answer, sir.

Mr. RASMUSSEN. Again, because I operate only in the Classified space, so it is difficult to answer in the Unclassified.

Mr. BARLETTA. I would like to thank you all of you for your testimony today. It was very helpful.

Thank you, Mr. Chairman.

Chairman MCCAUL. Thank you.

Mr. Loudermilk.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

I guess I am bringing up the rear here. First of all, thank you all for what you are doing to protect America. Very difficult time we live in. It seems like every committee—and I apologize I wasn't here for all the questioning. I listened to your statements, but another committee hearing dealing with vulnerabilities of our power grid. So it seems like most of the committees I am on is something dealing with security.

Question, I want to go back to the refugee situation. I apologize if I am redundant on some of the questions. I don't think they have been asked. But the concern I have, yes, we are a very humanitarian Nation, I think we do have some responsibility there. But our priority is securing this Nation and the people of this Nation. I have read reports that of the Syrian refugees, 72 percent of them are young males while 28 percent are women and children under the age of 11. The question I have for whoever has the information is, to your knowledge, is that true, and if it is not, what is the breakdown? If it is, why is there such a disparity?

Secretary JOHNSON. Congressman, I don't recall what the percentage breakdown is. I have heard a number, but I don't recall what it is. I don't know the accuracy of that 72, 28 percent number, but we can certainly get you what we know to be the case.

Mr. LOUDERMILK. Mr. Rasmussen.

Mr. RASMUSSEN. I am in the same position.

Mr. COMEY. The same.

Mr. LOUDERMILK. It is very concerning to me with that response that we are considering bringing in refugees, and we don't know that—what the breakdown of the percentage of these——

Secretary JOHNSON. Well, sitting here, I don't know. It is a piece of data that we have. I just don't know sitting here.

Mr. LOUDERMILK. All right. I appreciate the candor there.

How are we going to monitor these folks? I mean, I have also read reports that al-Qaeda, ISIS, have also said that their intention is to exploit the refugee crisis and to use that to infiltrate operatives into various countries. I mean, how are we going to monitor these folks? Do we have plans going forward?

Secretary JOHNSON. Congressman, as we discussed previously, there is that concern. We know that organizations such as ISIL might like to try to exploit this program, and it is for that reason that while we are going to do what we have committed to do for humanitarian reasons, you know, this is a world-wide crisis, we are talking about 10,000 people, I am committed that we do it carefully, and we vet these people as carefully as we can.

We live in a world where one failure is the equivalent of 10,000 successes. So, I think we are all committed, with the improved process we have, to do the best we can deliberately as we can with regard to each individual applicant for refugee status here.

Mr. LOUDERMILK. Do we have the resources to do this? Are we already stretched thin, and we are just going to be adding so much more to our vulnerabilities by going through this process?

Secretary JOHNSON. We are very busy. Our overall commitment in fiscal year 2015 was 75,000 world-wide. Next year—this year, we have committed to taking in a little more, 85, 10,000 of which will be Syrians. The director of USCIS has developed a plan along with the State Department to make sure we have adequate resources to vet these people.

Mr. LOUDERMILK. Of the—last question, and I yield back. I know we all have other things we need to be doing, but this is very critical.

Are we—do we have a system of prioritization? Like, we know that certain religious groups, Christians, for example, are the most at risk in some of these areas. Are we going to prioritize those that are greatest at risk to allow them in?

I have read reports that some of the Christian Syrian refugees are having a difficult time coming to the United States and some other countries. Is that true?

Secretary JOHNSON. I would have to get back to you and take that one for the record, sir.

Mr. LOUDERMILK. Okay. Well, I appreciate that.

Again, thank you for what you are doing. I am greatly concerned over where we are going with the refugee crisis.

Mr. Chairman, I yield back.

Chairman MCCAUL. If I could just add to that. It is unfortunate the Gulf states have not agreed to take one Syrian refugee. They are seeing the Arabs, and those are Sunni Arab populations. They certainly have the wherewithal.

But in closing, let me just say thank you to all three of you, and to the men and women in your organizations who every day wake up to protect Americans from the threats that we face. I think you have done an extraordinary job stopping so many of these threats, many that we know about, and many that the American people don't know about.

The challenges are enormous, and the threats are grave, but on behalf of the Congress, let me just say thank you, again, for what you do day in and day out.

With that, this committee stands adjourned.

[Whereupon, at 12:35 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE SCOTT PERRY FOR HONORABLE JEH C. JOHNSON

Question 1a. Last week, during a commencement speech at Stanford University, U.S. National security advisor Susan Rice, stated that "climate change is a direct threat to the prosperity and safety of the American people." In a hearing my subcommittee held earlier this year, it was noted that while the Department has released 13 strategic documents related to climate change—Quadrennial Homeland Security Review, Climate Change Adaptation Report, Climate Change Adaptation Roadmap, DHS Climate Action Plan, to name a few, only two—possibly a third—strategic documents related to countering violent extremism exist. In addition, while the Department requested $16 million on climate change activities for fiscal year 2016, there was no request to fund activities related to countering violent extremism. Does the Department consider violent extremism less of a direct threat to the prosperity and safety of the American people than climate change?

More specifically, how has the Domestic Nuclear Detection Office (DNDO) reacted or adjusted their focus, if at all?

Answer. DHS prepares for a multitude of threats and hazards (man-made and natural) that include the impacts of climate change and the threat of violent extremism. Violent extremism is neither limited by international borders nor to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence in the United States or against U.S. interests to try to force political, economic, or social change.

Our approach to countering violent extremism emphasizes the strength of local communities. Well-informed and well-equipped families, communities, and local institutions represent the best defense against violent extremists. While our primary purpose is to prevent a terrorist or violent extremist attack by an individual or group recruited by a violent extremist organization—or inspired by a violent extremist ideology—we also support stronger and safer communities as important ends themselves. This is a critical priority for all of DHS.

DHS has recently undertaken a number of actions to improve and prioritize CVE efforts further. In September 2015 we established the Office for Community Partnerships (OCP) OCP's mission is to "develop and implement a full-range of partnerships to support and enhance efforts by key stakeholders to prevent radicalization and recruitment to violence by terrorist organizations. The Office will leverage the resources and relationships of the Department of Homeland Security and apply the personal leadership of the Secretary to empower leaders in both the public and private sectors to spur societal change to counter violent extremism." OCP's major objectives are:

- *Philanthropic engagement*.—OCP will engage the philanthropic community to facilitate long-term partnerships with communities;
- *Tech sector engagement*.—OCP will engage the tech sector to empower credible voices in vulnerable communities against violent extremism;
- *Community engagement*.—OCP will conduct a community engagement roadshow that engages DHS Senior Leadership with vulnerable communities;
- *Field support expansion and training*.—OCP will strengthen and expand DHS field staff with training and connecting them to support local communities and front line law enforcement engaged in CVE efforts;
- *Grant support*.—OCP will work with FEMA to increase access to grants that support CVE initiatives.

Key stakeholders and partners working with OCP range from local law enforcement, to the private sector, to civil society. OCP works with local, State, Tribal, territorial, and Federal law enforcement by providing training, exercises, and technical assistance. Influential community leaders such as religious leaders, city councils, and local NGOs work directly with OCP field staff in identifying issues specific to that community, conducting CVE community exercises, and voicing concerns at com-

munity roundtables. Congress is supporting this effort, and in this year's spending deal, approved a $50 million grant program to be administered by DHS to address violent extremism, which includes up to $10 million allocated towards prevention efforts. The Office for Community Partnerships will use this $10 million to help non-Government efforts to counter violent extremism.

Further, the administration recently announced the creation of the Countering Violent Extremism Task Force, which is an interagency effort tasked with organizing Federal CVE efforts. The CVE Task Force will be hosted and led by DHS for the first 2 years; afterwards, the Department of Justice will assume leadership for 2 years, after which it is expected that leadership will rotate. It will consist of staffing from agencies and departments such as the Federal Bureau of Investigation and the National Counterterrorism Center. The main objectives of the interagency task force are:

- *Research and Analysis*.—The task force will coordinate Federal support for ongoing and future CVE research and establish feedback mechanisms for CVE findings, thus cultivating CVE programming that incorporates sound results.
- *Engagements and Technical Assistance*.—The task force will synchronize Federal Government outreach to and engagement with CVE stakeholders and will coordinate technical assistance to CVE practitioners.
- *Communications*.—The task force will manage CVE communications, including media inquiries, and leverage digital technologies to engage, empower, and connect CVE stakeholders.
- *Interventions*.—The task force will work with CVE stakeholders to develop multidisciplinary intervention programs.

DNDO remains singularly focused on the threat of radiological and nuclear terrorism, regardless of the cause. Our current analytical methodologies account for adversaries by their level of capability, which includes a span of possibilities from state-sponsored groups to lone actors. DNDO remains committed to understanding how the threat of radiological and nuclear terrorism will evolve in the future and ensuring our defensive investments are targeted appropriately. DNDO also remains committed to ensuring that the Nation maintains operationally-ready technical nuclear forensics capabilities so that the United States can hold fully accountable any State, terrorist group, or other non-state actor that supports or enables terrorist efforts to obtain or use radiological or nuclear weapons or materials out of regulatory control.

Question 1b. Has DNDO highlighted any gaps in the Global Nuclear Detection Architecture (GNDA) that could account for these recently-documented smuggling attempts?

Answer. DNDO views the recently documented disruptions of smuggling attempts to be positive examples of success for the layered defense upon which the Global Nuclear Detection Architecture (GNDA) is based. In particular, these examples highlight the international cooperation that DNDO and its interagency partners pursue on a daily basis. While gaps exist in the individual layers of the GNDA, DNDO works collectively to make the illicit acquisition, fabrication, and transport of a nuclear or radiological device or material an increasingly difficult endeavor for terrorists. In conjunction with our interagency colleagues, we continue to work with our international partners to bolster their defensive capabilities and improve the overall effectiveness of the GNDA.

Question 2a. Given the requirement for expediting Syrian refugee resettlements, are DHS assets adequate to conduct thorough security screening of refugee applicants?

Question 2b. Has USCIS engaged in additional cross-training opportunities with the IC?

Answer. The security vetting for refugees is the most robust screening process for any category of individuals seeking admission into the United States. The process is multi-layered and intensive, involving multiple law enforcement, National security, and intelligence agencies across the Federal Government. Additional enhancements have been added with regard to Syrian refugees. DHS and the Department of State continually evaluate whether more enhancements are necessary and coordinate with the intelligence and law enforcement communities.

All refugee applicants, including Syrians, may only be admitted to the United States after all security checks are completed. With every refugee application, the burden of proof is on the applicant to show that he or she qualifies for refugee status. The law requires refugee applicants to provide information that establishes their identity and allows U.S. Citizenship and Immigration Services (USCIS) to assess whether they present a security risk to the country. If USCIS does not have enough information to reach a sound decision, or if fact patterns evident in the case raise questions that are not satisfactorily addressed by the refugee applicant, the

refugee case is placed on hold until those issues can be resolved, or it is denied. Below is a detailed account of the vetting steps conducted for refugee applicants, including security checks, and multiple interviews.

For every refugee applicant, the Department of State conducts biographic checks of the refugee's primary name and any aliases against its Consular Lookout and Support System database (CLASS). CLASS includes watch list information from the Terrorist Screening Database (TSDB), the Drug Enforcement Administration, the Federal Bureau of Investigation's (FBI) Terrorist Screening Center, and Interpol, including criminal history, immigration history, and records of any prior visa applications submitted by the applicants. Significantly, for individuals meeting certain criteria, the Department of State also requests a Security Advisory Opinion name check against law enforcement and intelligence databases. In addition, the Department of State initiates an interagency check against intelligence community holdings, including the National Counterterrorism Center. These latter two enhanced biographic checks are conducted for all refugee applicants within a designated age range, regardless of nationality. These biographic checks do not occur only once, but are repeated throughout the vetting process to ensure that adjudicators consider the most up-to-date information available to the U.S. Government.

USCIS also collects biometric information, consisting of photographs and fingerprints, for refugee applicants of certain ages. USCIS coordinates the screening of refugee applicant fingerprints against the vast biometric holdings of the FBI's Next Generation Identification system, and DHS's Automated Biometric Identification System (IDENT). Through IDENT, applicant fingerprints are screened not only against watch list information, but also for previous immigration encounters in the United States and overseas—including, for example, cases in which the applicant previously applied for a visa at a U.S. embassy. Working with DHS, the Department of Defense (DOD) augments biometric screening on refugee applicants of all nationalities who fall within the prescribed age ranges by checking the fingerprints of refugee applicants against their own database.

In addition to biographic and biometric system checks, refugee applicants undergo a series of interviews including an interview with Department of State contractors who interview the applicant to confirm information about the case, collect identification documents, and obtain biographic data.

After this prescreening occurs, the case is referred to a highly-trained USCIS officer responsible for conducting refugee status interviews overseas and making the eligibility determination. In addition to the basic training received by all USCIS officers, refugee officers undergo 5 weeks of specialized and extensive training that includes comprehensive instruction on all aspects of the job, including refugee law, grounds of inadmissibility, fraud detection and prevention, security protocols, interviewing techniques, credibility analysis, and country conditions research. USCIS officers conduct extensive interviews with each refugee applicant to develop all relevant issues related to eligibility for refugee resettlement and admissibility to the United States. These interviews provide the U.S. Government a very useful tool for gathering information about a refugee applicant that may not already exist in a database. Officers receive additional training on country conditions and issues specific to the populations they will be interviewing. Before they may interview refugee applicants from the Middle East, USCIS has instituted Middle East-specific training for officers adjudicating cases with Iraqi and Syrian applicants. This training includes additional information on country conditions, armed groups operating in Iraq and Syria and a Classified briefing.

Additionally, USCIS Headquarters staff provides an additional level of scrutiny by reviewing all Syrian refugee applicant cases prior to the USCIS officer interview to identify potential National security concerns. For cases with potential National security concerns, USCIS Headquarters staff conducts both open-source and Classified research on the facts presented and synthesizes an evaluation for use by the interviewing officer. This information provides case-specific context relating to country conditions and regional activity and is used by the interviewing officer to develop lines of inquiry related to the applicant's eligibility and credibility.

Before an approved refugee arrives in the United States, U.S. Customs and Border Protection (CBP) at DHS receives a manifest of all refugees who have prior approval to travel to the United States. As part of CBP's Pre-Departure targeting operations, CBP gathers information and assesses risk and conducts pre-departure screening for all international flights arriving to the United States by commercial air. CBP receives this manifest in advance of a refugee's scheduled travel. The agency performs initial vetting before arrival at a Port of Entry and then conducts additional background checks of these subjects upon arrival. CBP Officers inspect and interview all refugees applying for admission to verify identity and admissibility as refugees.

A refugee applicant cannot be approved for travel and admission to the United States until all required security checks have been completed and cleared. Bottom line—under the current system, if there is doubt about whether an applicant poses a security risk, that individual will not be admitted to the United States as a refugee.

Question 3. USCIS adjudicators should be trained in interview techniques, common tactics used by fraudulent/deceitful actors, information gathering/verification methods, regional/cultural knowledge, and local linguistic trends (names/aliases) for translators.

Answer. Recognizing that a well-trained cadre of officers is critical to protecting the integrity of the refugee process, we have focused our efforts on providing the highest-quality training to our adjudicating officers. In addition to the basic training required of all USCIS officers, refugee officers receive 5 weeks of specialized training that includes comprehensive instruction on all aspects of the job, including refugee law, grounds of inadmissibility, fraud detection and prevention, security protocols, interviewing techniques, credibility analysis, and country conditions research. Before deploying overseas, officers also receive pre-departure training which focuses on the specific population that they will be interviewing. This includes information on the types of refugee claims that they are likely to encounter, detailed country of origin information, and updates on any fraud trends or security issues that have been identified. With the advent of large-scale processing of Iraqi applicants in 2007, USCIS officers who adjudicate Iraqi refugee applications began receiving additional 2-day training on country-specific issues, including briefings from outside experts from the intelligence, policy, and academic communities. This training has since expanded to a 1-week training in order to include Syria-specific topics as well.

In order to fully explore refugee claims and to identify any possible grounds of ineligibility, specially-trained USCIS officers conduct an in-person, in-depth interview of every principal refugee applicant. The officer assesses the credibility of the applicant and evaluates whether the applicant's testimony is consistent with known country conditions. These adjudicators also interview each accompanying family member age 14 and older to determine their admissibility to the United States. In addition, refugee applicants are subject to robust security screening protocols to identify potential fraud, criminal, or National security issues. All refugee status determinations made by interviewing officers undergo supervisory review before a final decision is made. Refugee Affairs Division policy requires officers to submit certain categories of sensitive cases—including certain National security-related cases—to Refugee Affairs Division Headquarters to obtain concurrence prior to the issuance of a decision. This allows for Headquarters staff to conduct additional research, liaise with law enforcement or intelligence agencies, or consult with an outside expert before finalizing the decision.

QUESTIONS FROM HONORABLE EARL L. "BUDDY" CARTER FOR HONORABLE JEH C. JOHNSON

Question 1. To what extent is the DHS working to address the National shortage of trained and educated cybersecurity professionals who are needed not only by Government, but by industry?

Answer. The Department leads the National cybersecurity public awareness, education, training, and workforce development efforts to create a more resilient and capable Nation, which includes not only the Government, but the private and nonprofit sectors as well. Through this work, the Department continues to support building resilient, cyber capable communities, to ensure current and future cyber operational requirements will be met through a skilled cybersecurity workforce.

The process of developing a strong, resilient cybersecurity workforce must begin before college.

As such, the Department issued the competitive Cybersecurity Education and Training Assistance Program (CETAP) grant to provide cyber education for middle school and high school teachers and students.

The CETAP grant supports development of cybersecurity-integrated middle school and high school curricula, which high schools across the country can adopt and offer to numerous students each year. The Department plans to leverage this curriculum and provide free, on-demand training to public school teachers Nation-wide through the Federal Virtual Training Environment (FedVTE). Using a virtual capability to reach teachers in any location, at any time, will provide for a tremendous flexibility to reach a broad audience. The curricula developed through CETAP are already free and available for download to all U.S. teachers.

The CETAP grant also provides cyber education summer camps, with the primary goal of educating high school teachers who return to their schools prepared to edu-

cate students on cyber-related content across multiple academic disciplines. Cyber education camps will be held in three communities in the summer of 2016, with more than 30 high schools participating. Upon completion of summer camp, the Department estimates each teacher will educate approximately 120 students over the course of an academic year.

DHS/NPPD also supports cyber competitions for middle school and high school students through its sponsorship of the annual Air Force Association CyberPatriot competition, steering participating students toward cybersecurity careers and studies. Since 2009, the program has experienced per annum growth of more than 20 percent.

At the college level, DHS partners with the National Security Agency (NSA) to co-lead the National Centers of Academic Excellence (CAE) program. The CAE program promotes higher education and research in Information Assurance and Cyber Defense, producing a growing pipeline of professionals with cybersecurity expertise in various disciplines. There are now over 191 academic institutions with CAE designation in 46 States, the District of Columbia, and Puerto Rico. CAE graduates fill cybersecurity roles across the country, including in the private sector.

DHS also partners with the National Science Foundation (NSF) and the Office of Personnel Management to co-sponsor the CyberCorps®: Scholarship for Service (SFS) program. The SFS program provides competitive awards to multiple colleges and universities with existing strong academic programs in cybersecurity to fund cybersecurity scholarships. Students receive SFS scholarships for up to 3 years to study cybersecurity, after which they must work for a Federal, State, local, or Tribal government organization in a position related to cybersecurity for a period of service equivalent to the length of their scholarship.

To train State and local law enforcement professionals, the Secret Service operates the National Computer Forensics Institute (NCFI). The National Computer Forensics Institute (NCFI), located in Hoover, AL, is a Federally-funded training center dedicated to instructing State and local law enforcement officers, prosecutors, and judges in digital/cyber crime investigations. The NCFI was opened in 2008 through collaboration between the U.S. Secret Service (Secret Service), the Department of Homeland Security (DHS), and the State of Alabama, with a mandate to provide State and local law enforcement, legal, and judicial professionals a free, comprehensive education on current cyber crime trends, investigative methods, and prosecutorial challenges. Its more than 4,000 students have included personnel from all 50 States, three U.S. territories, and over 1,500 agencies Nation-wide. The Secret Service plans to hold over 46 classes and train an estimated 1,200 personnel.

DHS Science and Technology Directorate (S&T) also supports cyber competitions for all ages through the U.S. Cyber Challenge, which presents on-line challenges focused on fundamental cybersecurity skills where the top scorers are invited to go to cybersecurity camps to participate in classroom learning. In addition, DHS S&T supported the development of the National Collegiate Cyber Defense Competition, where teams of college students are charged with maintaining and defending a business interest from concentrated, orchestrated attacks from a red team. DHS S&T is also engaged in building a community of cybersecurity professionals, private and public sector, to maintain and enhance their skills through competitions through the *http://cybercompex.org* portal, an on-line community focused on cybersecurity and cybersecurity competitions.

S&T is also supporting the development of a curriculum development tool for educators to create cybersecurity learning objectives in fun, easy-to-learn branching story-telling and knowledge checks.

In addition to supporting formal education initiatives, the Department also provides free on-line cybersecurity training through FedVTE. An on-line training platform, FedVTE provides Government cybersecurity and IT professionals with hands-on labs and training courses. Annually, FedVTE aids in addressing training gaps for more than approximately 60,000 cybersecurity professionals across the Government. The environment is accessible from any internet-enabled computer and is free to users and their organizations. This program saves the Federal Government approximately $72 million in training costs annually. Although originally intended for a Federal Government audience, DHS has recently granted access to State, local, Tribal, and territorial Government employees and to U.S. veterans.

Finally, the DHS National Initiative for Cybersecurity Careers and Studies (NICCS) portal represents a key component that promotes the National Cybersecurity Workforce Framework, which includes tools and resources for organizations focused on cybersecurity workforce and information for individuals about cybersecurity careers. The NICCS portal makes resources available to the American public, including the private sector, assisting users of all ages in locating cybersecurity learning opportunities and careers. The NICCS portal also hosts the National Cy-

bersecurity Training Catalog—a clearing house of cybersecurity or cybersecurity-related education and training courses offered across the United States; the Cybersecurity Workforce Development Toolkit—a guide to building an organization's cybersecurity workforce and provides easy access to the FedVTE training portal.

Question 2. Has DHS looked at partnering with academia like Armstrong State University in Savannah, Georgia to further assist in seeding growth to meet future needs of the Nation?

Answer. DHS partners with NSA to co-lead the CAE program, which enables collaboration with the nearly 200 colleges and universities with CAE designation. DHS/NPPD has directly partnered with CAEs in the past to further the cause of meeting the future needs of the Nation in cybersecurity. For example, in fiscal year 2012, DHS/NPPD funded projects at the University of Washington, Dakota State University, the University of Texas at San Antonio, and Mississippi State University to demonstrate the importance of cybersecurity in critical infrastructure protection.

Each academic institution with one or more CAE designations contributes significantly to the growth of a strong and dependable pipeline of cybersecurity employees, by providing interns and graduates who will enter the workforce armed with the most current and in-demand cybersecurity knowledge that employers seek. Further, to receive designation, each CAE must demonstrate that their cybersecurity curriculum maps to core and optional knowledge units, thus demonstrating that their curriculum meets the Nation's cybersecurity needs.

Although Armstrong State University is not currently a designated CAE, if Armstrong State University wishes to apply for CAE designation, its representatives should visit *https://www.iad.gov/NIETP/CAERequirements.cfm* to learn more about the program requirements.

Question 3. How does DHS engage with academic institutions, such as Armstrong State University, to encourage the adoption of best practices and find common solutions to our most pressing cybersecurity concerns?

Answer. DHS engages with academic institutions across the country, including in multiple States, the District of Columbia and the Commonwealth of Puerto Rico, primarily through its co-leadership of the CAE program. Through the CAE program, DHS interacts with nearly 200 community colleges and universities throughout the year at various events, such as cybersecurity education conferences, and at individual meetings with these schools. In addition, DHS contributes to the development and enhancement of core and optional knowledge units, which collectively standardize the curricula offered at these schools, thus ensuring that America's students receive the most rigorous and current cybersecurity educations possible. Further, DHS serves as a strategic advisor to the CAE program, including providing advice on the program's communication plans and growth strategy.

While an academic institution, such as Armstrong State University, need not have CAE designation for DHS to engage with it, by receiving CAE designation, Armstrong State would demonstrate that its cybersecurity curriculum meets the Government's needs in cybersecurity education and is among the top schools in the Nation in terms of its cybersecurity course offerings. If Armstrong State University wishes to apply for CAE designation, its representatives can visit *https://www.iad.gov/NIETP/CAERequirements.cfm* to learn more about the program requirements, and DHS personnel are available to speak to the University's representatives.

Another way that DHS engages with the academic community to encourage adoption of best practices and educate students about ways to be safe on-line is through the National Cybersecurity Awareness Campaign, Stop.Think.Connect. Academic Alliance. The Stop.Think.Connect. Campaign is a National public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure on-line.

Through the Academic Alliance, DHS and the Campaign share vital resources and information to partners, stakeholders, students, and community members across the country at a variety of academic institutions.

Currently, there are over 50 Academic Alliance partners that have joined the Campaign partnership through DHS to date. These universities and colleges join 150 additional partners from non-profit organizations and Government agencies/departments committed to increasing on-line safety. This collaboration allows all partners to obtain cybersecurity tips, messaging, articles, and presentations, gain access to DHS Campaign materials, tools, and subject-matter experts, and join monthly partner discussions highlighting current cyber issues and trends.

The Stop.Think.Connect. Campaign provides the Academic Alliance partners with beneficial insight into cyber threats that fellow academic institutions face as well. They also join monthly partner calls that highlight resources and information from non-profit partners and partners from Federal/local government agencies and de-

partments. In addition, these partners plan outreach activities throughout the year across the country, including focused cybersecurity awareness activities during National Cyber Security Awareness Month, which takes place each October.

In August 2000, the Secret Service and CERT, part of the Software Engineering Institute (SEI), a Federally-funded research and development center (FFRDC) located at Carnegie Mellon University, established the Secret Service CERT Liaison Program. The purpose of the liaison program is to provide technical support, training, opportunities for research and development. Through this partnership with CERT, the Secret Service extends its investigative capabilities through the efforts of more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training, and education.

The Secret Service leverages CERT's innovative technology and expert staff to meet emerging investigative and protective challenges. To meet emerging challenges to investigative operations, the Secret Service sponsors the development of forensic tools available for use by law enforcement, military, and intelligence agencies. CERT provides support to complex electronic crime investigations in the areas of forensic analysis, network traffic analysis, cryptanalysis, malicious code analysis forensic tool development and training development.

DHS also partners with the National Science Foundation (NSF) and the Office of Personnel Management to co-sponsor the CyberCorps: Scholarship for Service (SFS) program. The SFS program provides competitive awards to multiple colleges and universities with existing strong academic programs in cybersecurity to fund cybersecurity scholarships. Students receive SFS scholarships for up to 3 years to study cybersecurity, after which they must work for a Federal, State, local, or Tribal government organization in a position related to cybersecurity for a period of service equivalent to the length of their scholarship. This program is specifically called out and funding is required by the Department in appropriations language.

Additionally, the U.S. Secret Service operates a cyber facility housed on the University of Tulsa, a CyberCorps SFS program school, wherein SFS students work with Special Agents of the Secret Service toward a three-pronged mission: (i) Training Federal, State, and local law enforcement agents in mobile device forensics; (ii) developing novel hardware and software solutions for extracting and analyzing digital evidence from mobile devices; and (iii) applying the hardware and software solutions to support criminal investigations conducted by the Secret Service and its partner agencies.

Question 4. Does the agency have any plans to increase cooperation with the academic community moving forward?

Answer. DHS is actively engaged with the academic community in terms of information sharing and collaboration on projects that support the DHS mission. For example, the DHS Office of Academic Engagement formed the Homeland Security Academic Advisory Committee (HSAAC), which advises DHS on matters related to the five DHS mission areas from an academic perspective. HSAAC includes a cybersecurity subcommittee.

Although cooperation between DHS and the academic community is strong, DHS is always seeking opportunities to expand and enhance this cooperation. For example, DHS is very interested in expanding the number of CAE-designated institutions to include at least one designated CAE in all 50 States. Further, DHS is looking to expand the number of CAE focus areas, ensuring that more CAEs are able to become certified in cybersecurity areas that support DHS's mission critical needs. DHS is actively seeking the support and interest of academic institutions to reach to local high schools and middle schools to encourage adoption of cyber-integrated curricula. Finally, DHS will continue to build its awareness and general cyber outreach efforts with academia.

Question 5. What is DHS doing to synchronize these efforts and adopt a combined approach to address an evolving cyber threat landscape?

Answer. Cybersecurity is a shared mission and requires coordinated efforts among Government, the private sector, and academia to effectively manage both current and emerging risks. DHS executes coordination with academia through three principal mechanisms. First, DHS, within its National Protection and Programs Directorate (NPPD), maintains a Cybersecurity Education and Awareness program office that is responsible for synchronizing education and workforce development across the cybersecurity community. By centralizing education and workforce activities within a single program office, NPPD promotes broad and systemic adoption of common standards and curricula. The Centers for Academic Excellence (CAE) program exemplifies this approach, as NPPD is able to synchronize cybersecurity programs across over 200 higher education institutions through guidance, accreditation, and workforce opportunities for eligible students.

Second, NPPD's National Cybersecurity and Communications Integration Center (NCCIC) serves as the U.S. Government's 24/7 hub for cybersecurity information sharing, incident response, and coordination. Thirteen Federal departments and agencies and 16 private-sector entities have regular, dedicated liaisons at the NCCIC, while over 100 private-sector entities collaborate and share information with the NCCIC on a routine basis. The NCCIC shares information on cyber threats and incidents, and provides on-site assistance to victims of cyber attacks. In this year alone, the NCCIC has shared over 15,000 bulletins, alerts, and warnings, responded on-site to 21 incidents and conducted nearly 130 technical security assessments. The NCCIC allows DHS to adopt a combined approach in bringing together government, the private sector, and international allies in addressing a shared cyber threat.

Third, NPPD leverages the National Infrastructure Protection Plan (NIPP) to work with critical infrastructure partners across the country. Recognizing that critical infrastructure is increasingly dependent on cyber space for the provision of key services and functions, NPPD works to align physical and cybersecurity services to work with the private sector in developing and promulgating sector- and organization-specific guidance, in turn promoting the adoption of common best practices that are sufficiently flexible to address the unique business and risk environments of individual organizations.

Question 6. How hard would it be to tie in cyber activities at the Federal Law Enforcement Training Center in Brunswick, GA with the capabilities pioneered by universities like Armstrong State in the cyber forensics realm?

Answer. To ensure its training continues to meet the needs of today's law enforcement officers and agents, the Federal Law Enforcement Training Centers (FLETC) must incorporate expertise and technological advances born from academia, industry, military, and law enforcement in its cyber training programs. As innovation is not exclusive to one specific individual or entity, FLETC partners with a diverse cross-section of experts to ensure it maintains current knowledge and expertise in the critical area of cyber forensics.

FLETC participates in discussions with a variety of Government and non-Government committees and groups that share thoughts and ideas related to cyber crime. Through these organizations, FLETC has opportunities to discuss tools, techniques, and training standards with other cyber experts, which often leads to FLETC incorporating new material into its cyber-related training. The following are professional organizations FLETC presently partners with in sharing and developing cyber training, which also partner with academia:

- Computer Crime and Digital Evidence Committee for the International Association of Chiefs of Police, National Center for Forensics Science at the University of Central Florida
- Department of Homeland Security, Science and Technology Directorate, Cyber Forensics Working Group, Centers of Excellence with multiple universities including the University of South Carolina, the University of Minnesota, and the University of Illinois
- Federal Bureau of Investigation Cyber Shield Alliance and Cyber Investigator Certification Program, Software Engineering Institute of the Carnegie Mellon University
- INTERPOL Global Cybercrime Expert Group.

FLETC also partners with the following organizations, primarily consisting of law enforcement, which routinely share ideas with academia about cyber tools and techniques:

- National Technical Investigators Association
- Defense Cyber Investigations Training Academy
- High Technology Crime Investigations Association
- International Association of Computer Investigative Specialists
- Computer Crime and Intellectual Property Section of the United States Department of Justice.

Periodically, FLETC meets with academic institutions to discuss cyber curriculum and to share information. FLETC has conducted cyber training for law enforcement at the campuses of Armstrong Atlantic State University and the University of Central Florida. A faculty member from each university participated in the session on his or her respective campus. Additionally, FLETC is currently partnering with the College of Coastal Georgia (CCGA) by sharing curriculum development expertise as CCGA pursues designation as a Center of Academic Excellence in Information Assurance/Cyber Defense. This partnership allows both organizations to share best practices, exposes FLETC staff to related university-level processes, and facilitates increased access by CCGA to associated FLETC subject-matter experts. Since 2007 FLETC has hosted 7 college interns in its Cyber Division. These students conducted

research projects and attended training in a variety of law enforcement topics. FLETC would welcome the opportunity to expand its collaboration with academia on cyber training in the interest of ensuring its training curriculum is up-to-date and meets the needs of today's law enforcement officers and agents.

QUESTIONS FROM HONORABLE BARRY LOUDERMILK FOR HONORABLE JEH C. JOHNSON

Question 1a. There have been varying data reports on the ratio of men to women and children coming into our borders. Most of the statistics I have come across indicate that the majority of Syrian refugees are predominately males while a small percentage remains women and children. Is this true?

Question 1b. If so, what is the correct ratio of Syrian refugee men to women and children?

Answer. The overwhelming majority of Syrian refugees we have accepted and will accept are families, children, and other especially vulnerable refugees, such as victims of torture and those with medical needs or disabilities. We have prioritized the most vulnerable of Syrian refugees for resettlement—which include those who are victims of the violence perpetrated by both the Assad regime and ISIL in Syria.

Of the overall caseload of Syrian refugees referred to the U.S. Refugee Admissions Program (USRAP), that caseload is evenly split between male and female applicants (53 percent male and 47 percent female). Over 50 percent of applicants are 18 years of age or younger; approximately 2.5 percent of the applicants are over the age of 60; and fewer than 2 percent of the applicants are unattached single males with no cross-referenced cases and no relatives or friends in the United States. For information regarding refugees resettled in the United States, we would refer you to the Department of State.

Question 2. As we welcome an additional 10,000 Syrian refugees in fiscal year 2016 alone, how are you and your partner agencies planning to monitor admitted refugees to ensure violent extremists have not infiltrated their ranks?

Answer. Refugees undergo a rigorous screening process prior to their admission into the United States. The process is the most robust for any category of individuals seeking admission into the United States, and is multi-layered and intensive. It involves multiple law enforcement, National security, and intelligence agencies across the Federal Government. Only those satisfying these rigorous requirements are admitted into the United States as refugees.

Refugee status is a permanent immigration status and a person admitted as a refugee is authorized to remain in the United States indefinitely barring any negative information such as criminal history or loss of immigration status. A person admitted as a refugee is required to apply for adjustment of status to lawful permanent residency 1 year after being admitted to the United States. Five years after arrival a refugee can apply for naturalization, provided they have adjusted status to permanent resident during this time, continuously resided in the U.S. for 5 years prior to applying for naturalization, submit to security checks, and meet the other eligibility requirements for naturalization.

Like other residents of the United States, refugees enjoy freedom of movement within the country. Refugees, like other non-citizens, are required to report any change-of-address to USCIS within 10 days of moving within the United States or its territories. As noted, a refugee is also required to apply for adjustment of status to permanent residence status 1 year after admission as a refugee. At this point, security checks are re-run and the applicant is questioned again about potential grounds of inadmissibility, such as criminal activity or terrorism-related inadmissibility grounds. Finally, any refugee who comes to the attention of law enforcement or National security agencies may be subject to criminal charges or civil immigration proceedings, possibly leading to removal from the country.

Question 3. Is the United States prioritizing Christian refugees, who are focal persecution targets in Syria?

Answer. When referring cases to the U.S. Refugee Admissions Program, the U.N. High Commission for Refugees and Department of State emphasize the most vulnerable Syrians, including female-headed households, children, survivors of torture, and individuals with severe medical conditions. Members of religious minorities, including Christians, may be among those referred as vulnerable refugees.

QUESTIONS FROM HONORABLE NORMA J. TORRES FOR HONORABLE JEH C. JOHNSON

Question 1. What specific steps have the Department of Homeland Security, FBI, and NCTC taken to ensure its respective workforces reflect the diversity of the communities they protect?

Answer. DHS issued a Diversity and Inclusion Strategic Plan in fiscal year 2012 that specifically provides the framework for recruiting a diverse workforce, creating

an inclusive workplace, and ensuring management accountability. The Office of the Chief Human Capital Officer coordinates Departmental efforts to recruit from a diverse, broad spectrum of potential applicants, including a variety of geographic regions, academic sources, and professional disciplines. Each DHS operational component completes an annual Component Recruiting and Outreach Plan that identifies short and long-term workforce needs, including workforce diversity. To the extent practical, we coordinate specific recruiting efforts collaboratively. We also maintain a consolidated recruitment presence on our website.

Question 2. What are your respective diversity goals and what is the time frame for achieving those goals?

Answer. DHS (and other Federal agencies) are not permitted to have diversity goals in terms of hiring, except with hiring veterans and individuals with disabilities. For all other groups, DHS analyzes the workforce diversity of each component and works on recruiting and outreach strategies for groups with low participation rates.

Question 3. Have DHS, FBI, and NCTC engaged in outreach efforts to high school and post-secondary schools to inform students about careers in homeland security and intelligence?

Answer. The Department of Homeland Security (DHS) maintains several dedicated outreach initiatives and partnerships with academic institutions to promote the Department's mission to various academic communities. Two DHS Headquarters programs focus on engagement with the academic community:

- In 2011, DHS established the Office of Academic Engagement (OAE) to build and strengthen the Department's relationship with the academic community. Among its responsibilities, OAE manages the Homeland Security Academic Advisory Council, a Federal advisory committee of college and university presidents, academic leaders, and interagency partners that provides advice and recommendations to the Secretary on topics related to homeland security and the academic community, including cybersecurity and student and recent graduate recruitment.
- In 2013, the Department established the CyberSkills Management Support Initiative (CMSI), addressing recommendations from the Homeland Security Advisory Council's Task Force on CyberSkills. CMSI's main purpose is to develop and execute Department-wide human capital strategies, policies, and programs that will create, enhance, and support a top-notch DHS cyber workforce. CMSI works directly with secondary and post-secondary institutions to provide students with information regarding DHS's cybersecurity mission and workforce opportunities.
- In 2014, DHS OCHCO executed Memoranda of Understanding (MOU) with five higher education associations representing more than 1,500 colleges and universities, including community colleges and minority-serving institutions. Through the MOUs, DHS engages the associations to provide information on employment and internship opportunities for students and recent graduates. DHS meets with the associations semiannually and provides quarterly reports to the associations on employment and grant opportunities. Also as a result of the MOUs, in 2015, DHS representatives participated in National conferences of the Hispanic Association of Colleges and Universities and the Asian American and Pacific Islander Association of Colleges and Universities to share information on employment opportunities at DHS.

As the number of students studying technical and cyber-related majors has increased, the Department recognizes that academic institutions and student groups provide access to a large talent pool for cybersecurity positions. These outreach events build partnerships with 2-year and 4-year academic institutions, as well as K–12 schools to connect classroom coursework to real-world cybersecurity careers. The Department uses several approaches to connect with academic institutions and students, including:

- Launching the Secretary's Honors Program Cyber Student Volunteer Initiative (CSVI) in 2013. CSVI allows students pursuing cybersecurity-related degrees at 2- and 4-year colleges and universities the opportunity to gain hands-on experience at DHS through temporary volunteer opportunities. CSVI initially started as a pilot program with 21 participants, who worked with U.S. Immigration and Customs Enforcement in 18 cities Nation-wide. The 2014 CSVI cohort expanded to 7 participating Components with 70 student volunteers placed in 40 DHS office locations. In 2015 the cohort included 8 participating components that placed 51 volunteers in 31 DHS offices in 20 States.
- Conducting cybersecurity-focused panel discussions and tours with academic institutions at various DHS component locations attended by DHS executive leadership.

- Hosting webinars with colleges and universities informing students of DHS career opportunities and the Department's commitment to engaging cyber talent to build a cybersecurity workforce.
- Developing the National Initiative for Cybersecurity Careers and Studies (NICCS) portal, an on-line resource for Government, industry, academia, and the general public to learn about cybersecurity awareness, education, careers, and workforce development opportunities.
- Sponsoring the CyberCorps®: Scholarship for Service (SFS) program through the National Protection and Programs Directorate (NPPD). SFS provides scholarships through the National Science Foundation to 56 universities across the country. Selected students receive SFS scholarships for up to 3 years to study cybersecurity, after which they owe the Government a period of service equivalent to the length of their scholarship.
- Sponsoring the CyberPatriot competition, which impacts numerous middle and high school students each year and steers them toward cybersecurity careers and studies. Since 2009, this NPPD program has experienced per annum growth of more than 20 percent. Teams from all 50 States and the District of Columbia participate in CyberPatriot.
- Sponsoring the National Collegiate Cyber Defense Competition where more than 2,000 students representing over 180 colleges and universities competed in a scenario-based defense competition.
- Supporting the U.S. Cyber Challenge, where approximately 2,000 students compete on-line for a scholarship and a chance to attend 1 of 4 week-long cybersecurity training camps throughout the Nation.
- Regularly conducting outreach to schools to inform students about careers in homeland security intelligence through the Office of Intelligence and Analysis (I&A). In fiscal year 2015, I&A participated in 13 outreach events at universities and colleges Nation-wide. Two of these events were in concert with intelligence community partners, including the Federal Bureau of Investigation and National Counterterrorism Center. In September 2015, I&A also supported a Congressional Black Caucus event designed to increase diversity in Government that included high school and post-secondary students.

Question 4. What obstacles stand in the way of your respective agencies hiring a workforce that represents the diversity of the United States?

Answer. The DHS civilian workforce is very diverse. In fiscal year 2015, 43 percent of the workforce self-identified as other than white (non-Hispanic) compared to 35 percent for the Federal Government overall. Hispanics comprise nearly 21 percent of the DHS civilian workforce, compared to the 8 percent for the Federal workforce overall. DHS is committed to a diverse and inclusive workforce, and efforts to create a diverse workforce remain a special focus for the Department's recruitment efforts.

DHS is the Nation's largest law enforcement agency; almost 40 percent of positions across DHS are law enforcement-related. DHS is committed to greater outreach to women regarding career opportunities in law enforcement. This commitment is demonstrated by strong partnerships with professional organizations for women law enforcement, ensuring broad DHS engagement in high-profile recruiting events focusing on women and women in law enforcement in particular, and various component-lead best practices including targeted marketing campaigns. Specific examples include:

- strong coordination with Women in Federal Law Enforcement (WIFLE) organization and at WIFLE annual training conferences
- attendance at Women's Leadership Symposium and Women Veterans Employer Symposium
- OCHCO partnering with CBP regarding Border Patrol Agent and CBP Officer recruitment and hiring, with a focus on transitioning service members, veterans, and women and
- marketing in Professional Woman's Magazine Spring 2015 Issue and *WomenforHire.com.*

In addition, in fiscal year 2015, the President's Council on Veterans Employment (Council) asked the DHS CHCO to lead an interagency workgroup on Women Veterans. The workgroup's final report and recommendations were adopted by the Council and now apply to all 24 agencies under the Executive Order. The White House reviewed the report and issued a blog on the Joining Forces website and requested OPM to publish the report on the "Feds Hire Vets" website. In fiscal year 2016, OCHCO will assemble a DHS-wide workgroup to develop a broader strategy on recruitment of women for law enforcement, which will also include a specific focus on women veterans.

Competition with other Federal agencies and the private sector for the same talent is the primary obstacle in creating and sustaining a workforce that fully reflects the diversity of the United States. For some high-demand positions such as cybersecurity and science, technology, engineering, and math (STEM), DHS competes for top talent with not only other Federal agencies, but the private sector as well. DHS is working to enhance the pool of available diverse talent in these types of fields through its utilization of the Pathways Programs; the Secretary's Honors Program; Cyber Student Volunteer Initiative; and MOUs with Higher Education Associations. DHS shares information about employment opportunities with Higher Education Associations such as Hispanic Association of Colleges and Universities (HACU); National Association for Equal Opportunity in Higher Education (NAFEO); American Indian Higher Education Consortium (AIHEC); Asian Pacific Islander American Association of Colleges and Universities (APIACU); and the American Association of Community Colleges (AACC). DHS is also partnering with the White House Office of Science and Technology Policy, OPM, and 13 other Federal agencies to increase diversity in STEM across the Federal Government. DHS also utilizes mechanisms such as direct hire authority for cybersecurity positions, an authority which OPM recently extended at the Department's request. DHS is actively working on the long-term implementation of cybersecurity-specific hiring and pay flexibilities which Congress granted to the Secretary in the Border Patrol Agent Pay Reform Act.

QUESTIONS FROM HONORABLE BARRY LOUDERMILK FOR NICHOLAS J. RASMUSSEN

Question 1a. There have been varying data reports on the ratio of men to women and children coming into our borders. Most of the statistics I have come across indicate that the majority of Syrian refugees are predominately males while a small percentage remains women and children. Is this true?

Answer. Response was not received at the time of publication.

Question 1b. If so, what is the correct ratio of Syrian refugee men to women and children?

Answer. Response was not received at the time of publication.

Question 2. As we welcome an additional 10,000 Syrian refugees in fiscal year 2016 alone, how are you and your partner agencies planning to monitor admitted refugees to ensure violent extremists have not infiltrated their ranks?

Answer. Response was not received at the time of publication.

Question 3. Is the United States prioritizing Christian refugees, who are focal persecution targets in Syria?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE NORMA J. TORRES FOR NICHOLAS J. RASMUSSEN

Question 1. What specific steps have the Department of Homeland Security, FBI, and NCTC taken to ensure its respective workforces reflect the diversity of the communities they protect?

Answer. Response was not received at the time of publication.

Question 2. What are your respective diversity goals and what is the time frame for achieving those goals?

Answer. Response was not received at the time of publication.

Question 3. Have DHS, FBI, and NCTC engaged in outreach efforts to high school and post-secondary schools to inform students about careers in homeland security and intelligence?

Answer. Response was not received at the time of publication.

Question 4. What obstacles stand in the way of your respective agencies hiring a workforce that represents the diversity of the United States?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE SCOTT PERRY FOR JAMES B. COMEY

Question 1. Earlier this month, the Associated Press reported that in the past 5 years, the FBI has thwarted four smuggling attempts of nuclear and radioactive material in Eastern Europe—with the latest occurrence in February of this year. With the knowledge of this thriving "nuclear black market," what is the administration's plan to counter this threat?

Answer. Response was not received at the time of publication.

Question 2. What are the FBI's plans for the influx of expected Syrian refugees?
Does the FBI anticipate that the influx of Syrian refugees will present a burden on existing manpower and resources?
Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE EARL L. "BUDDY" CARTER FOR JAMES B. COMEY

Question 1. What is the FBI doing to target terrorist groups that use the internet to prey on young Americans?
Answer. Response was not received at the time of publication.
Question 2. Are we using social media to engage communities to recognize when a young individual might be a target to a terrorist group?
Answer. Response was not received at the time of publication.
Question 3a. What is being done specifically to work on the community level to address the issue of targeting young adults?
Are we talking with clergy?
Are we doing town hall meetings?
Is law enforcement making themselves available on a daily basis?
Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE BARRY LOUDERMILK FOR JAMES B. COMEY

Question 1a. There have been varying data reports on the ratio of men to women and children coming into our borders. Most of the statistics I have come across indicate that the majority of Syrian refugees are predominately males while a small percentage remains women and children. Is this true?
Question 1b. If so, what is the correct ratio of Syrian refugee men to women and children?
Answer. Response was not received at the time of publication.
Question 2. As we welcome an additional 10,000 Syrian refugees in fiscal year 2016 alone, how are you and your partner agencies planning to monitor admitted refugees to ensure violent extremists have not infiltrated their ranks?
Answer. Response was not received at the time of publication.
Question 3. Is the United States prioritizing Christian refugees, who are focal persecution targets in Syria?
Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE NORMA J. TORRES FOR JAMES B. COMEY

Question 1. What specific steps have the Department of Homeland Security, FBI, and NCTC taken to ensure its respective workforces reflect the diversity of the communities they protect?
Answer. Response was not received at the time of publication.
Question 2. What are your respective diversity goals and what is the time frame for achieving those goals?
Answer. Response was not received at the time of publication.
Question 3. Have DHS, FBI, and NCTC engaged in outreach efforts to high school and post-secondary schools to inform students about careers in homeland security and intelligence?
Answer. Response was not received at the time of publication.
Question 4. What obstacles stand in the way of your respective agencies hiring a workforce that represents the diversity of the United States?
Answer. Response was not received at the time of publication.