

**CYBERSECURITY, TERRORISM, AND BEYOND:
ADDRESSING EVOLVING THREATS TO THE
HOMELAND**

HEARING

BEFORE THE

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

SECOND SESSION

SEPTEMBER 10, 2014

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

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



U.S. GOVERNMENT PUBLISHING OFFICE

92-903 PDF

WASHINGTON : 2015

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan	TOM COBURN, Oklahoma
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE McCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	MICHAEL B. ENZI, Wyoming
TAMMY BALDWIN, Wisconsin	KELLY AYOTTE, New Hampshire
HEIDI HEITKAMP, North Dakota	

GABRIELLE A. BATKIN, *Staff Director*

JOHN P. KILVINGTON, *Deputy Staff Director*

HARLAN C. GEER, *Senior Professional Staff Member*

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

KEITH B. ASHDOWN, *Minority Staff Director*

CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*

WILLIAM H.W. MCKENNA, *Minority Investigative Counsel*

DANIEL P. LIPS, *Minority Director of Homeland Security*

LAURA W. KILBRIDE, *Chief Clerk*

LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Carper	1
Senator Coburn	3
Senator Johnson	18
Senator McCain	20
Senator Baldwin	22
Senator Portman	25
Senator Ayotte	28
Prepared statements:	
Senator Carper	35
Senator Coburn	37

WITNESSES

WEDNESDAY, SEPTEMBER 10, 2014

Hon. Francis X. Taylor, Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security; and Hon. Suzanne E. Spaulding, Under Secretary, National Protection and Programs Directorate, U.S. De- partment of Homeland Security	6
Nicholas J. Rasmussen, Deputy Director, National Counterterrorism Center, Office of the Director of National Intelligence	9
Robert Anderson, Jr., Executive Assistant Director, Criminal, Cyber, Re- sponse, and Services Branch, Federal Bureau of Investigation, U.S. Depart- ment of Justice	13

ALPHABETICAL LIST OF WITNESSES

Anderson, Robert Jr.:	
Testimony	13
Prepared statement	57
Rasmussen, Nicholas J.:	
Testimony	9
Prepared statement	47
Taylor, Hon. Francis X.:	
Testimony	6
Joint prepared statement with Ms. Spaulding	38

APPENDIX

Information submitted by Senator Baldwin	64
Responses to post-hearing questions for the Record:	
Mr. Taylor and Ms. Spaulding	72
Mr. Rasmussen	92

CYBERSECURITY, TERRORISM, AND BEYOND: ADDRESSING EVOLVING THREATS TO THE HOMELAND

WEDNESDAY, SEPTEMBER 10, 2014

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

The Committee met, pursuant to notice, at 9:32 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Baldwin, Coburn, McCain, Johnson, Portman, and Ayotte.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Good morning, everyone. Great to see you. Welcome, and we thank you for joining us and look forward to your testimonies.

Almost every year, this Committee holds a hearing to review a multitude of threats to our homeland and examine how our government is working to counter those threats. We routinely hear from the Department of Homeland Security (DHS) and we hear from the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC) about how we can best keep Americans safe from those who would seek to carry out deadly attacks against our country and its people. We also hear about actors in cyberspace that want to drain our bank accounts, who want to shut down our financial systems, our electric grid, steal our individually identifiable information and our identities, as well as the Research and Development (R&D) that will enable American businesses and our military to remain pre-eminent in the world.

Assessing these ever-changing, broad threats and making sure our government continues to hone its ability to stop them remains a top priority for this Committee, particularly as we approach another September 11, 2001 anniversary. This year, our hearing takes on an added significance as our Nation confronts a growing terrorist threat in Iraq and Syria. As we sit here today, our military is engaging in limited air strikes in Iraq in an effort to dislodge and repel that threat. Later this evening, President Obama will address our Nation. He is expected to share with us and the world the steps that he is recommending be taken in Iraq and in Syria to reverse the expansion of the Islamic State of Iraq and

Syria (ISIS) and to enable the people who live in those countries to reclaim their lives.

Much of the world has been exposed to a steady stream of deeply disturbing images from those regions in recent weeks: brutal executions, human rights atrocities, repression of women, and a seemingly endless procession of masked militants defiantly waving the black flag of jihad in celebration of their brutality.

Effectively addressing the threat from the newly proclaimed Islamic State will require a multifaceted strategy, and that strategy will need a military component and the development of a robust international coalition to execute it. Among the goals of that strategy is to ensure that the Islamic State of Iraq and Syria does not establish a long-term safe haven from which it can launch attacks against either our allies or our homeland—much like we saw al-Qaeda do in the days before September 11, 2001.

Today we will examine the steps that our Federal Government has already taken, along with the steps that we still need to take, to prevent this from happening. We will drill down on this threat and its impact on our homeland, both in this open hearing as well as in a classified briefing directly following. But that is not all we are going to do. In addition to examining the more conventional terrorist threats the instability in Iraq and Syria may pose, we will also closely examine another major threat that affects our homeland, and that is, daily cyber attacks.

Every day nation states and their affiliates—criminals, terrorists, and hackers—launch cyber attacks against our government agencies, our businesses, and important parts of our daily lives such as utilities and financial networks. Some of these actors want to steal our sensitive information to sell it on the black market or to gain a competitive edge. Others are trying to make a political point. Some, however, would like to use a cyber attack to cause wide-scale economic damage or even physical harm. Many of them are good at it, and they are getting even better. We need to stay a step ahead of them. Today we will hear in the open portion of this hearing and also in the closed portion how we plan to do that, not unlike the steps we have taken to address terror threats in the wake of September 11, 2001.

Congress clearly has a role to play here. Actually, several roles. One of them is an oversight role. It is one that we take very seriously. Another is a legislative role that involves developing legislation to help enable America to anticipate and repel the cyber attacks that we face on an almost daily, 24/7 basis today. In the last several months, this Committee has completed action and reported three separate cyber bills unanimously to the full Senate. One bill would significantly enhance the capabilities of the Department of Homeland Security's cyber workforce. Another would better protect Federal agencies from cyber attack. And a third would codify the cyber center that the Department of Homeland Security uses to monitor and respond to attacks to strengthen its ability to do so. I am grateful to Dr. Coburn and his staff for working closely with us on each of those pieces of legislation.

Yesterday in an op-ed in *The Hill* newspaper, Secretary Johnson recognized the bipartisan efforts of this Committee, and he talked about the critical need to pass cyber legislation this Congress. I

could not agree more. In closing, as we mark the anniversary of September 11, 2001 tomorrow, let us keep in mind one of the key lessons we learned since that fateful day some 13 years ago, and that is, the threat is always evolving. Not that long ago, crooks used to rob a bank to steal our money. Now they click a button on a distant computer and accomplish the same goal. Nation states and rival businesses used to employ corporate insiders or retirees to steal company secrets. Now they send a spear-phishing e-mail. And terrorists used to be a distant threat in the mountains in places like Afghanistan or Pakistan. Now an increasing number of them are homegrown. They may be using European, or even, American passports.

So as the threat becomes more sophisticated, more elusive, and more diffuse, we need to remain ever vigilant to ensure that our government is nimble enough to keep up with tomorrow's threats as they confront us. We have come a long way since September 11, 2001. In many respects, we are more secure than we were on this day 13 years ago. But the world in which we live remains a dangerous place. There is always more work to do. When it comes to securing our homeland and anticipating the next threat, we owe it to the American people to strive for perfection.

What does it say in the Preamble of the Constitution? "In order to form a more perfect union." It was not the idea to form a perfect union, but to form a more perfect union. And our intent here is to try to approach perfection, even if we never achieve it, but get as close as we can in this regard. The consequences of failure are simply too high, and the costs are too severe.

I am pleased that we have with us today a panel of witnesses who work together every day to tackle the terrorist and cyber threats that we face. We are grateful to each of you for what you do with your life and for your service to our country.

Now I turn to my partner in all this, Dr. Coburn, for any remarks that he might wish to make. Dr. Coburn.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Well, thank you, Mr. Chairman. I concur with a lot of what you said. I want to thank each of our witnesses today for their testimony—one, for what you do; two, for your vigilance; and three, for the criticism you take that is actually not informed criticism.

The Department of Homeland Security particularly had lots of problems. I am so thankful Jeh Johnson is there. General, I am thankful you are there, and, Suzanne, I am thankful for you there, plus the others that we put through the Committee.

We have a long way to go. Where I would disagree with Senator Carper is I do not think we are any safer today. I think the threat to our country is just as great as it was pre-9/11 based on what is happening in the world; the absolute lack of control of our border, especially our Southern border, and the inability and the corruption on both sides in terms of law enforcement on the border. So I think we have a long way to go, but I know we have dedicated leadership now in all the areas that are concentrating on the same goal.

I think it is a shame that the leader of the Senate will not put a cybersecurity bill on the floor, one that creates true information sharing. Let the Senate debate it so we can actually start to really protect the cyber aspect of our government. And that requires all of us to work together in the cyber realm to ensure that we are not vulnerable. We are vulnerable today. We have seen both in Homeland Security and in the private sector significant breaches. Most of them are on nation state actors, China and Russia specifically. We should not fall back from talking about what they are doing and why they are trying to both steal our intellect and damage our economy.

These are real issues. This is an important hearing for the American people to hear, in as much detail as possible, what is going on and where we need to improve.

So, again, I would thank you all for your efforts, the FBI and NCTC, and valuable contributions. And having the privilege of sitting on both Intel and Homeland Security, I get to see as well as anybody what everybody is doing, and everybody is working in the right direction except the U.S. Senate. And my hope would be that we would start helping you rather than hurting you.

I yield back.

Chairman CARPER. I would like to associate myself with the remarks of my colleague from Oklahoma. We need to move not just the three cyber bills that have been reported out of this Committee, I think unanimously, but also some version of the information-sharing bill. I think we can improve the bill that came out of the Intel Committee, and my hope is that we will and we will have a chance to do all four of them, at least those four, this year. That is my goal. If we can do more, God bless us.

On behalf of all the Members of our Committee, thank you for joining us today.

Our first witness is retired Brigadier General Francis Taylor. Mr. Taylor is the Under Secretary for Intelligence and Analysis in the Department of Homeland Security. How long have you been in that job now, General?

General TAYLOR. Four months, sir.

Chairman CARPER. Four months, good. In this role he provides the Secretary, DHS leadership, DHS components, and State, local, tribal, and private sector partners with the homeland security intelligence and information they need to keep our country safe, secure, and resilient. General Taylor came to DHS with 31 years of service in the U.S. Air Force, 4 years in the State Department as Counterterrorism Coordinator and as the Assistant Secretary for Diplomatic Security, and 8 years as vice president at General Electric.

The second witness is Suzanne Spaulding, the Under Secretary for National Protection and Programs Directorate (NPPD) at the Department of Homeland Security. As Under Secretary, one of her responsibilities is coordinating and overseeing policy and operation for the Department's infrastructure protection activities, including cybersecurity. Ms. Spaulding has spent more than 25 years working on national security issues in Congress, in the Executive Branch, and in the private sector. This includes extensive experience working with many critical infrastructure sectors. Welcome.

Our next witness is Nick Rasmussen, Deputy Director of the National Counterterrorism Center for the Office of the Director of National Intelligence. Mr. Rasmussen has also served on the National Security Council where he was responsible for providing staff support to the President, the National Security Adviser, and the Homeland Security Adviser on counterterrorism policy and strategy. Prior to this he served in a variety of key positions for the Department of State where he provided support for the Arab-Israeli peace process, the U.S.-North Korean Agreed Framework, and Persian Gulf security issues. Nick, welcome this morning.

And our final witness is Robert Anderson, Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch of the Federal Bureau of Investigation. In this position Mr. Anderson oversees all FBI criminal and cyber investigations worldwide, international operations, critical incident response, and victim assistance. During the 20 years that he has worked at the FBI, Mr. Anderson has served in the Hostage Rescue Team, Counterintelligence Division, and the Intelligence Division as well.

What did you do before you were part of the FBI?

Mr. ANDERSON. Sir, I was a Delaware State trooper for almost 9 years.

Chairman CARPER. No kidding. Were you any good?

Mr. ANDERSON. I hope so.

Chairman CARPER. Were you ever Trooper of the Year?

Mr. ANDERSON. Yes, sir, I was, in 1989.

Chairman CARPER. OK. That is pretty good. We remember you fondly.

Senator COBURN. Did you ever escort the former Governor of Delaware?

Chairman CARPER. He pulled me over. [Laughter.]

He pulled me over a time or two. And as I recall, one other time fired a warning shot. [Laughter.]

No damage was done. Great to see you, and thanks for what you did for us back in Delaware and what you are doing for your country now.

Thank you all for your service. Your entire testimonies will be made part of the record, and we would ask you to try to give your testimony in about 5 minutes. If you go way over that, we will pull you in.

All right. General Taylor, feel like leading us off?

TESTIMONY OF HON. FRANCIS X. TAYLOR,¹ UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY; AND HON. SUZANNE E. SPAULDING, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

General TAYLOR. Yes, sir. Thank you, Chairman Carper, Ranking Member Coburn, distinguished Members of the Committee. Thank you for the opportunity to appear before you today to discuss threats to the homeland and the current threat environment. I am mindful that tomorrow is September 11, and I vividly remember where I was on that day 13 years ago, sitting at the State Department as the coordinator for counterterrorism.

What has changed since 2001? Are we any safer now? These are questions that have been repeated countless times since that tragic day, and rightfully so. I come before the Committee today to outline the lessons we have learned since September 11, 2001, and how we are now postured to address evolving threats in ways that we were not on September 10, 2001.

The lesson we have learned from September 11, 2001 is the need to develop an agile homeland security enterprise that constantly collaborates and shares information and intelligence, to identify threats and risks, and to adjust operations as necessary to address the range of challenges the Nation faces.

The partners within the homeland security enterprise, whether they are first responders at the local level of decisionmakers in capital cities across America or here in our Nation's capital, require predictive intelligence and analytical products that help them to make informed decisions to protect our citizens.

The cornerstone of our mission at DHS has always been, and remains, protecting the Nation against terrorist attacks. In fact, Secretary Johnson just yesterday reiterated that counterterrorism is our most important mission at DHS. We are vigilant in detecting and preventing terrorist threats that may seek to penetrate the homeland from land, sea, or air. I will first address the current terrorist environment and then discuss threats to our efforts as they relate to each of the Secretary's four priorities. And, Mr. Chairman, mindful of the time limit, I will submit other remarks for the record and summarize just a couple of things.

First, on terrorism, Core al-Qaeda, al-Qaeda in the Arabian Peninsula (AQAP), and their affiliates remain a major concern for the Department of Homeland Security. Despite senior leadership deaths, the groups maintain the intent and capability to conduct attacks against U.S. citizens and facilities, and have demonstrated the ability to adjust their tactics, techniques, and procedures for targeting the West in innovative ways.

The Islamic State of Iraq and the Levant (ISIL) is a terrorist group operating as if it were a military organization, and their experience and successes on the battlefields of Syria and Iraq have armed them with capabilities most terrorist groups do not possess. At present, DHS is unaware of any specific, credible threat to the

¹The joint prepared statement of Mr. Taylor and Ms. Spaulding appears in the Appendix on page 38.

U.S. homeland from ISIL. However, we recognize that ISIL constitutes an active and serious threat within the region and could attempt attacks on U.S. targets overseas with little or no warning.

ISIL exhibits a very sophisticated propaganda capability, disseminating high-quality media content on multiple online platforms, including social media, to enhance its appeal. Media accounts of the conflict, and the propaganda in particular, play a role in inspiring U.S. citizens to travel to Syria. We are aware that a number of persons—more than 100—have either made their way or tried to make their way to Syria over the past few years to join the international foreign fighters.

I will conclude that AQAP has attempted three times to attack the U.S. homeland. The airliner plot of December 2009, an attempt against the U.S.-bound cargo planes in October 2010, and an airline plot in May 2012 demonstrate their efforts to adapt to aviation security procedures and underscore why aviation security is a priority area outlined by Secretary Johnson.

In response to these recent threats, generally from overseas, over the past few months, DHS has taken steps to enhance aviation security at overseas airports with direct flights to the United States. And other nations have followed suit with similar enhancements.

Mr. Chairman, I will conclude my remarks, and if you would, allow me to submit the rest of them for the record.

Chairman CARPER. Without objection, your entire statement will be made part of the record. Thank you, General.

Ms. Spaulding, great to see you. Please proceed.

Ms. SPAULDING. Thank you, Chairman, Ranking Member Coburn, distinguished Members of the Committee. Thank you for this opportunity to be here today. I am particularly pleased to be here today with my colleague, Under Secretary Taylor, and with our partners from the Federal Bureau of Investigation and the National Counterterrorism Center.

Under Secretary Taylor spoke with you about a range of threats that the Department is focused on, and I am going to amplify a bit with regard to the threat to cybersecurity and to discuss the actions that we are taking with our critical infrastructure partners to understand and address these threats, both physical and cyber, through information sharing and capability building.

First, however, I also want to note, as we approach this 13th anniversary of the attacks of September 11, 2001, three efforts that we have underway to heighten public vigilance and public awareness. This month, September, is National Preparedness Month. October is National Cybersecurity Awareness Month in which we focus on enhancing the resilience of this Nation against cyber threats. And November is Critical Infrastructure Security and Resilience Month. All three of these are key mission areas for the Department, and all require daily collaboration with our stakeholders in the private sector and government at all levels.

Growing cyber threats are an increasing risk to critical infrastructure, to our economy, and to our national security. DHS uses cybersecurity information to reduce risk, to detect and block cyber attacks on Federal civilian agencies, to help critical infrastructure entities improve their own protection, and also to use the information that we develop collaboratively to protect their customers; and

we maintain a trusted environment for the private sector partners to collaborate on cybersecurity threats and trends. This trust is based in large part on our commitment to privacy, civil rights, and civil liberties across all information-sharing programs, with a particular emphasis on safeguarding personally identifiable information.

So far this year, DHS' 24x7 cyber operations center, the National Cybersecurity and Communications Integration Center (NCCIC), has processed over 600,000 cyber incidents, issues more than 10,000 actionable alerts, detected more than 55,000 vulnerabilities, and dispatched over 78 incident response teams for onsite technical assistance.

Let me tell you about one recent success. Within the last few weeks, the United States Secret Service shared information on some malware with our Cybersecurity Ops Center for analysis. The results of that analysis formed the basis for an actionable alert that was distributed widely to our critical infrastructure owners and operators and led U.S. businesses to check their systems for this malware and identify and stop ongoing cyber intrusions, thereby protecting their customers' data.

While both the cybersecurity threat and the Nation's dependence on cyber infrastructure has grown exponentially, the legal framework, particularly regarding the articulation of the Department's authorities, has not kept pace. As the Chairman and the Ranking Member have noted, legislative action is vital.

Both the House and the Senate have made real progress on cybersecurity legislation. I would like to personally thank this Committee for all of its hard work that has ensured progress on this front on a bipartisan basis.

But we are not over the finish line yet. As Secretary Johnson wrote today, there are areas of legislation with strong consensus: codifying the cybersecurity responsibilities of the Department of Homeland Security, making it easier for DHS and the private sector to work together to mitigate cyber-related vulnerabilities, and enhancing the Department's ability to recruit and retain that essential cybersecurity workforce. These authorities are vital to ensuring that the Department has the tools it needs to carry out its mission on behalf of the Nation.

While deliberations continue on other elements of cybersecurity legislation, we should not wait to pass bipartisan and broadly supported bills. You have come so far, and the threat is so great. I urge Congress to pass what it can now, even as we continue to work hard on remaining provisions.

Let me close by emphasizing that DHS' mission to strengthen the security and resilience of critical infrastructure requires us to focus on physical risks to that infrastructure as well as cyber risks. Because the majority of the Nation's critical infrastructure is owned and operated by the private sector, DHS works with those partners, primarily on a voluntary basis, to understand the range of threats and hazards, share information, and promote training and other capability building.

DHS and the Department of Energy, along with other inter-agency partners, for example, provide classified and unclassified threat briefings—we do this on a regular basis—to energy Chief

Executive Officers (CEOs) and industry executives on physical and cyber threats.

In the wake of the terrorist attack on the shopping mall in Nairobi, Kenya, DHS and the FBI engaged more than 400 major malls across the United States to facilitate tabletop exercises based on a similar attack involving active shooters and the use of improvised explosive devices (IEDs). Working collaboratively with our partners in the private sector, we are advancing our core mission of strengthening the security and resilience of our Nation's critical infrastructure against cyber and physical threats.

Chairman Carper, Ranking Member Coburn, thank you for this opportunity to testify today, and I look forward to taking your questions.

Chairman CARPER. Thank you. Thank you very much, Suzanne. We look forward to asking a few of them, too.

Mr. Rasmussen, welcome aboard. Please proceed.

TESTIMONY OF NICHOLAS J. RASMUSSEN,¹ DEPUTY DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. RASMUSSEN. Thank you, Chairman Carper, thank you, Ranking Member Coburn, and the Members of the Committee for the opportunity to testify here today.

NCTC Director Matt Olsen and I do not often testify in open hearings, and so today is an important opportunity, we believe, to share our understanding of what we see as an evolving, dynamic terrorist threat, and to share that understanding with the Committee and with the American public. Indeed, earlier in the summer, the 9/11 Commissioners challenged national security leaders to communicate more regularly with the American public about the threat, and we hope to do just that.

As I begin this morning, I would like to frame this evolving threat in broad terms that are generally applicable across the broad sweep of groups, of individual groups and terrorist networks. The threat from terrorist groups that we see today is geographically diffuse, from a diverse array of actors, and it is proving over time to be both resilient and adaptive to the counterterrorism pressure we are putting on it.

The global jihadist movement continues to increasingly decentralize itself, both in terms of geography and in terms of command and control. Geographically speaking, it is no longer generally confined to the Afghanistan-Pakistan-South Asia region. It now covers a broad swath of territory from the Indian subcontinent, across the whole entire Middle East and the Levant, and throughout northern Africa and western Africa as well.

Of greatest concern are the terrorist groups such as ISIL that have taken a foothold in areas where governance is lax, where governments are unable to govern, and where lax security has allowed groups to coalesce, train, and plot.

In terms of command and control, we also see a trend of decentralization, with the emir of an al-Qaeda affiliate, AQAP, now serving as the general deputy to al-Qaeda leader Ayman al-Zawahiri.

¹The prepared statement of Mr. Rasmussen appears in the Appendix on page 47.

Additionally, that al-Qaeda Core is increasingly encouraging groups and individuals to act independently in support of the global movement, with no longer holding an expectation that regional affiliates will discuss or clear their operational plans with al-Qaeda senior leadership prior to execution. And this evolution is the result of an adaptive enemy.

Our counterterrorism operations continue to degrade al-Qaeda's core ability to lead the global terrorist movement and to plan sophisticated attacks from its place in the Fatah. But as a result of leaks and disclosures, including those attributable to Edward Snowden, terrorists now understand the scope and scale of Western collection capabilities, and they are changing the way they communicate. They are adopting encryption technologies. They are shifting accounts or avoiding altogether the use of electronic communications, all of which frustrate our counterterrorism efforts. In short, we cannot connect the dots if we cannot collect the dots that matter the most, and our collection is challenged in this new environment.

In the remaining time, Mr. Chairman, I would like to focus on three specific areas: the threat from ISIL, the threat of AQAP, and the threat we face from homegrown violent extremists (HVE).

Starting with ISIL, the greatest threat from ISIL to the United States and its interests is inside Iraq right now, which, combined with Syria, constitutes ISIL's power center. As we move further from that base of strength, ISIL's ability at present to develop and execute significant, large-scale, sophisticated attacks diminishes. This is not to say it does not pose a threat outside the region. It certainly does. Indeed, the arrest in France of an individual and the subsequent discovery of explosive devices in his possession, as well as the killing of four individuals at a Jewish museum in Belgium provide clear evidence and indication of ISIL's ambition to operate outside the Middle East. Both of the responsible individuals, apprehended in Europe, who are in custody, reportedly fought alongside ISIL elements in the Middle East.

However, these examples also demonstrate that right now ISIL's ability to carry out complex, large-scale attacks in the West is currently limited. Left unchecked, however, that capability is likely to grow and present a much more direct threat to the homeland.

And with over 2,000 Westerners now believed to be fighting in Syria and Iraq, we assess that the threat to Europe is perhaps even more immediate. But, nevertheless, the United States is not immune, as both the Chairman and the Ranking Member noted.

Over 100 persons from a variety of backgrounds and from all across the country have traveled or attempted to travel or somehow indicated intent to travel to the region, including some who have looked to engage with ISIL. Most of these individuals are known or believed to have Western travel documentation that would ease their re-entry into the United States or into other countries, which is why identifying them is a top priority for the United States and our partners.

That is why it is so important that the international community challenge ISIL's regional ambitions now, degrade their capabilities, and over time work together to defeat and destroy ISIL. Left unchecked, ISIL poses an increasing threat to all governments it con-

siders apostate, not just to the United States or European nations, but also Middle Eastern, South Asian, and African nations as well.

Let me quickly turn to al-Qaeda in the Arabian Peninsula. We continue to assess that AQAP remains the al-Qaeda affiliate most likely to attempt transnational attacks against the United States. The group's repeated efforts to conceal explosive devices to destroy aircraft demonstrate its continued pursuit of high-profile attacks against the West, its increasing awareness of Western security procedures, and their efforts to adapt to those procedures that we adopt.

The group also continues to present a high threat to U.S. personnel and facilities inside Yemen and Saudi Arabia, and at any one time we are tracking several plots to our interests inside Yemen and inside the Arabian Peninsula hatched by al-Qaeda in the Arabian Peninsula.

The group also continues, as the Committee well knows, its efforts to radicalize and mobilize individuals outside Yemen through the use of Inspire Magazine, their English language publication. The most recent issue, its 12th issue of Inspire, was released back in March, and it continued to encourage lone wolf or lone offender attacks on the West, citing specific targets in the United States, the U.K., and France.

Let me also say a few quick words about homegrown violent extremists. The boundless online virtual environment we see today combined with terrorists' increasingly sophisticated use of social media makes it increasingly difficult for us to protect our youth from messaging that is designed to radicalize and motivate to action homegrown violent extremists. We at NCTC are working very closely with our partners at DHS, at FBI, and the Department of Justice to inform and equip families, communities, local governments, and local institutions, all of whom provide the best offense and have the greatest ability to counter the narrative of violent extremism in their communities.

Despite our efforts, however, HVEs remain the most likely immediate threat to the homeland, individual action by individual HVEs. We expect the overall level of HVE activity to remain about the same as what we have seen in recent years over the course of the next year, and by that I mean we would expect to see a handful of uncoordinated and mostly unsophisticated plots emanating from a pool of HVEs that amounts up to a few hundred individuals.

Last year's Boston bombing certainly underscored the threat from HVEs who were motivated, often with little or no warning, to act violently by themselves or in small groups. And as we have discussed with this Committee, these lone actors who act autonomously are the most difficult to detect or disrupt.

Mr. Chairman, during your April 30 hearing, you noted that identifying and deterring terrorist plots by lone wolves was extremely challenging to the counterterrorism and homeland security community, and I think everybody here would agree with that assessment.

Last, let me take one moment to talk about just one of our efforts at NCTC to counter the array of threats I have just outlined, and that is through identifying it more precisely, by putting a face and a name to that threat whenever possible. As you know, under the

law, NCTC is charged with maintaining the United States Government's central and shared knowledge bank of known and suspected terrorists as well as their contacts and their support networks.

NCTC's Terrorist Identities Datamart Environment (TIDE), is our database of known and suspected international terrorists, and it helps us ensure that all relevant information collected by the government about identified individuals, including individuals who we have identified as Syrian foreign fighters. All that information is shared with appropriate intelligence, law enforcement, and screening agencies. We are absolutely relentless in the efforts to ensure that the data in TIDE is as accurate as possible, that it is entered accurately, and that our records are as comprehensive as they can possibly be. And we are mindful of privacy and civil liberties concerns, particularly with respect to U.S. persons.

In the case of U.S. persons, any nomination to TIDE goes through at least four layers of review, including a legal level of review, to ensure that the underlying derogatory information is sufficient and meets established legal standards.

Our management at NCTC of this unique consolidation of terrorist identities has created a valuable forum for identifying and sharing information with our partners in the community, and it has better integrated our collective efforts to identify, enhance, and expedite the nomination of individuals we assess to be Syrian foreign fighters and get their names and their identities into the screening system. And this work greatly increases the chances that we will be able to disrupt potential terrorist activity by individuals as they seek to return from Syria.

In closing, Mr. Chairman and Members of the Committee, we face an evolving, decentralized threat from a diffuse set of actors who are adapting constantly to our countermeasures. That is why NCTC and our partners within the intelligence community (IC) must ourselves continue to adapt to this threat, operating within the bounds of our existing authorities and resources. We certainly appreciate the Committee's continued strong support in these efforts, and I would encourage Senators to visit NCTC to see firsthand the breadth of the work we are doing with our counterterrorism partners.

Mr. Chairman, we had the honor of hosting you and several of the Committee staff in recent weeks out at NCTC to talk in great detail about some of those threats, and it was very gratifying to see your interest in the work we are doing, along with the FBI and DHS.

Thank you again for this opportunity.

Chairman CARPER. Thank you. And can I mention that Dr. Coburn and I not only enjoyed being with you and having a chance to personally meet many of the folks who work there, but to thank them for their service. It was informative for me and, frankly, quite encouraging. So thanks for that.

Mr. Anderson, it is great to see you. Welcome. Please proceed.

TESTIMONY OF ROBERT ANDERSON, JR.,¹ EXECUTIVE ASSISTANT DIRECTOR, CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. ANDERSON. Thank you, Mr. Chairman, Ranking Member Dr. Coburn, and Members of the Committee. Thanks for the opportunity to be here today to talk to you about the cyber and terrorism threats to our Nation and how we are working together with our partners to prevent and combat them.

In my role as the Executive Assistant Director of the FBI, as the Chairman said, I manage multiple divisions within the FBI, but the two I am going to concentrate on the most today is the criminal and the cyber program.

As the Committee knows, the number of sophisticated cyber attacks against our Nation's network have increased dramatically over the recent years. We truly expect them to continue to climb and grow. I could break down the threats to our country in four broad categories from cyber: spies, transnational organized criminals, terrorists, and hactivist groups.

The bottom line is we are losing a lot of data, money, ideas, and innovation to a wide range of cyber adversaries. FBI Director Comey has recognized this, and the severity of the threat has made cyber one of the No. 1 top priorities in the FBI. Under his leadership, the FBI is continuing to strengthen our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of September 11, 2001.

Today's FBI is a national security and law enforcement organization that uses intelligence to prevent and respond to all types of threats. We constantly seek to understand the threats we face in each of our offices, both here and abroad, what is out there, what we see, and what we might be missing.

We know that to effectively combat the cyber threat, we must continue to expand our partnerships both in government and in the private sector. In fact, we expect Director Comey and DHS Secretary Johnson will soon sign a new cyber unified message for State and local law enforcement. This message makes clear that Federal agencies are working together to ensure that a call to one is a call to all when law enforcement partners report information on a cyber attack or incident.

Also, for our law enforcement partners, we launched the Cyber Shield Alliance, an online, one-stop shop to provide cyber training as well as the ability to report cyber incidents to the FBI.

Earlier this month, we deployed a malware repository and analysis system known as Malware Investigator. It allows our intelligence and law enforcement partners to submit malware directly to the FBI, and we share with our partners for triage and analysis of what is going on in cyber.

We are also significantly enhancing our collaboration with the private sector. In the past, industry has provided us information about attacks. We have investigated them, but we really did not share or provide that information back. Now we are.

¹ The prepared statement of Mr. Anderson appears in the Appendix on page 57.

As part of our enhanced outreach, we have provided nearly 40 classified sector-specific threat briefings to private companies over the past year alone. Over the past several months, the FBI and the Department of Justice (DOJ), along with many partners both at this table and abroad, have announced a series of indictments of cyber criminals. Just to name a few: Encore Performance, which was obviously the indictment of the five People's Liberation Army (PLA) Chinese hackers; Blackshades, a remote access computer software that could steal and infect hundreds of thousands of computers around the world. We are calling these indictments "the new normal" because we expect them to continue on a regular basis.

While the cyber threat is one of the FBI's highest priorities, combating terrorism continues to be the No. 1 priority in the FBI. As conflict zones continue to emerge throughout many parts of our world, we expect terrorist groups to use this instability to recruit and incite acts of violence.

Syria remains a major concern as the ongoing conflict shows no sign of subsiding. Due to the prolonged nature and the high visibility of the Syrian conflict, we are concerned that U.S. persons with an interest in committing jihad will be drawn to that region of the world. We can address these issues much more fulsomely in the closed session that follows this session, and we look forward to doing that.

In conclusion, Mr. Chairman, to counter the threats we face, we are engaging in an unprecedented level of collaboration within the U.S. Government and with our private sectors around the world and with the international law enforcement organizations that we each at this table talk to every day. We look forward to continuing to expand these partnerships and to work with the Committee to defeat our cyber and terrorist adversaries.

Thank you again very much for the opportunity to be here today. I would be happy to answer any questions you or the Committee may have. Thank you.

Chairman CARPER. Mr. Anderson, thanks so much. Great to see you. Thanks so much for joining us today.

The first question from me would be for perhaps Mr. Rasmussen or General Taylor. One of the recurring themes in my life is find out what works and do more of that. And I just want to play off of that for a moment.

Go back about 7 years ago, Iraq, Sunni Awakening, and the predecessor to ISIS was rolling along pretty well, and then not so much. And under the enlightened leadership of General Petraeus, I think the good work done by the fellow who has just become the new Prime Minister of Iraq, working with the Sunni tribal leaders, al-Qaeda in Iraq, the progress just stopped and was greatly diminished, pushed back.

What can we gain from that lesson? Is there anything there that can inform what we do today?

Mr. RASMUSSEN. Mr. Chairman, one of the things we have tried to do as we have tried to think about the problem and the threat posed by ISIL is to think of potential vulnerabilities that the group has and to think of ways in which the progress that they have made can be addressed. And you point to some of the lessons that we may be able to learn from previous efforts against al-Qaeda in

Iraq, and there I think we did learn that the group very much struggled to gain legitimacy across the broader population of Iraq when that population in Iraq saw in Baghdad a representative government that was responsive to their needs. And so the ongoing transition in Baghdad that you are seeing right now that you just alluded to I think is an important step in potentially giving the Sunni population in Iraq a signal that they do not have to turn or align or ally with ISIL in order to have their issues addressed, to feel that they are represented, that their interests are protected inside Iraq.

So that is an important lesson learned. I think it is one where we have seen progress in the last few weeks. But only over time will we see if that kind of political transition actually has that effect that we are looking to see. I do not know that we can say yet how quickly that will happen, but it is something that I think was a necessary precondition to any strategy against ISIL.

Chairman CARPER. Thanks very much.

General Taylor and maybe for you, Nick, one or both of you mentioned that the ability for ISIS to mount an effective attack against our homeland is limited, but it is not time for us to sit back and just assume it is not going to come, but for us to prepare and be ready for it. What are some ways that we can do, are doing, or should be doing to prepare for that eventuality and be better prepared for what should come? That would be for both of you. General Taylor, why don't you lead it off, and then we will give Nick some time as well, please.

General TAYLOR. Certainly, sir. As I mentioned, we assessed the threat from ISIL primarily to be in the region. Nonetheless, with the number of Europeans and Americans that have gone to fight in Syria, that threat can manifest itself back either in Europe or in the United States. I think we have begun with the aviation security changes that we have made since July to make it more difficult for people to try to get explosives onto aircraft, to bring those aircraft down that could be traveling to the United States. We have increased our intelligence cooperation with our partners across the world in attempting to identify people who have gone to serve or to fight in Syria, because intelligence is the one thing that helps us identify these individuals before they are able to act, and using our intelligence systems to learn who they are makes us much more effective in interdicting them.

And, third, I think the focus on Countering violent extremists (CVE), homegrown violent extremist, getting our communities aware of the risks—

Chairman CARPER. Thank you.

General TAYLOR. As Nick mentioned, probably the most immediate threat comes from a homegrown violent extremist who listens to the propaganda, reads it, and decides that he or she is going to answer the call and take up arms here in the United States. And so community awareness, resilience around these issues with our law enforcement partners in the field so that they understand what those elements are and to look for them as they encounter folks in communities I think is a big step toward helping communities learn about this early so we can respond.

Chairman CARPER. OK. Thanks. Nick.

Mr. RASMUSSEN. The only thing I would add, Mr. Chairman, are two things—one related to offense and one related to defense. I think if you are going to get ahead of ISIL's effort to over time develop a homeland threat capability, we have to over time shrink the safe haven and attack the safe haven inside Iraq. And that is something I know the President and the Secretary of State have already spoken about in talking to our foreign partners overseas, because absent that, the ability to bring additional Western potential operatives into Iraq or Syria into that safe haven and potentially train, equip, and deploy them back out to Europe and the United States will remain a threat.

The more defensive piece of business that I think we are engaged in right now already and I think we are making good progress on is just aggressive information sharing with all of our foreign partners who face a similar problem. This is an issue we have been engaged in with them for going on 18 months now, engaging with our European partners, many of whom face this problem even more acutely than we do in terms of their citizens having an easier route and certainly easier path to travel to Syria and Iraq.

Unlike a lot of situations where it is difficult to talk with partners about information sharing about individuals, this is a case where we are actually getting very little pushback. They share the same sense of threat, and so the information that we are able to share about individuals who have traveled to Syria or Iraq can be used to potentially add to our watchlisting and screening systems and give us a significant leg up in our effort to disrupt travel when those individuals seek to leave Syria and Iraq.

That is not a fail-safe. It is by no means the only pillar of a defensive effort, but it is an important pillar, and it is one that is not always very easy to get our partners to work with us on. But in that case, that sense of shared threat is so widely shared at all levels in the governments that we typically work with in Europe that it is making that level of interchange much more robust than it often is.

Chairman CARPER. Thanks very much. My time has expired. When we come back, either for a next round or maybe in our closed session, Ms. Spaulding and Mr. Anderson, I want to visit the issue of information sharing and the sequencing of Foreign Intelligence Surveillance Act (FISA) reauthorization information sharing, either in the open session or the closed session. Dr. Coburn.

Senator COBURN. Well, thank you. I hope the media that is here today actually listened to what you had to say, Nick, a very cogent, open assessment of where we are—not on the basis to scare people but on the basis to inform them of where we really are. I think the other thing that I would comment on is I am really happy to see the FBI being aggressive on deterrence because for so long we thought we could build a higher and higher wall that people cannot climb over. They are going to climb over every wall on cyber that we have. And we have to have both efforts. We have to have the wall, but we also have to have the prosecutorial deterrence that says you come at us, it is going to be painful.

And so I am very thankful for that attitude coming from the FBI. I hope to see more and more and more, both domestically and internationally, because of the costs.

General Taylor, let me just ask you a couple of questions. Has Intelligence and Analysis (I&A) produced any intelligence product examining the vulnerabilities in the Immigration and Customs Enforcement (ICE's) student exchange and visitors program, the visa program, and whether it poses a threat to national security?

General TAYLOR. Yes, sir, we have. We have published several threat pieces to support the student visa program and the risk that comes from that particular program, working with ICE and with the Customs and Border Protection (CBP).

Senator COBURN. And are those public, or are those classified?

General TAYLOR. I believe they are classified, Senator Coburn, but I will check and get back to you.

Senator COBURN. I will ask more questions about them in the closed hearing.

It is reported that millions of people are living here on visa overstays. The Government Accountability Office (GAO) has found that DHS is really struggling to track this population. We understand that. Has I&A prepared any assessment of the threat from the population of visa overstays? Do you have anything that you have done on that?

General TAYLOR. We have, sir. We have helped ICE to prioritize its focus on the visa overstays from a threat perspective and certainly can share that with you in the closed session.

Senator COBURN. All right. CBP has been very cooperative, by the way. When we review the documents, what we see today is approximately 700 miles of our Southern border that are not secure. That is looking at the documents that you all give us. Can you all prepare a current assessment of the coverage of the border and the threat to national security posed by adversaries that potentially might transcend that border?

General TAYLOR. Sir, if I understand your question, you are asking can we—or have we?

Senator COBURN. I am asking you can you, given the basis of where we stand?

General TAYLOR. Absolutely, yes, sir. I would also add, sir, that the Secretary has directed a comprehensive Southern border security strategy which will have an intelligence annex to it that will address what you have just described, the risks to the border and how we can better focus our efforts at securing those gaps that we identify exist.

Senator COBURN. Do you have a timeline on that?

General TAYLOR. He just approved it, at least the concept, and we are beginning to put meat on the bones. I cannot give you an exact date, but I will certainly have the staff check and get back with you.

Senator COBURN. All right. Thank you.

Mr. Anderson, does the FBI monitor cyber attacks against the Federal Government?

Mr. ANDERSON. Yes, sir, we work to not only monitor cyber attacks around the world with the Federal Government but also the private sector.

Senator COBURN. OK. Can you tell me which departments, major departments of the Federal Government, that have not been hacked?

Mr. ANDERSON. I do not know if I could tell you that off the top of my head, sir. I would probably have to go back and look. I would say—and I think I agree with our current Director—that if they have not been hacked—I do not know if they have not been hacked or we have not realized that—

Senator COBURN. They have all been hacked, yes. If you could go back and give us a list of what your records show?

Mr. ANDERSON. Sure.

Senator COBURN. And you can do that either in the secured setting or in an open session, but I would like to see what you all see on that. I mentioned the deterrence. I am really pleased with that because I think you have to have both sides of the sword working.

The rest of my questions, I think, Mr. Chairman, are for the classified setting, so I will wait and ask those of Nick and Suzanne and others in the classified session.

Chairman CARPER. Thank you. And the order of joining us at the hearing: Senator Johnson, Senator McCain, Senator Baldwin, Senator Portman, and Senator Ayotte. Senator Johnson, you are recognized.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman. I would like to associate myself with Senator Coburn's comments about the need for us to face this reality, the need for the American people to be informed. It is not about scaring people. It is about facing reality.

General Taylor, we started the hearing asking, Are we safer? I want to break that question down to two parts, because I think there are two parts to it. One is: Do we have greater defensive capability to keep us safe? But, then, has the threat grown?

I just want your assessment of both of those. What is your assessment over the last 13 years in terms of our defensive capabilities? And, by the way, what is hampering our efforts? And then really your assessment of the growing threat.

General TAYLOR. Thank you, Senator. As I mentioned, I was State Department Coordinator for Counterterrorism on September 11, 2001, and was party to our efforts then and have watched the government change its approach to this. Indeed, I think our capacity to share information, to work together, is as good as it has ever been in the history of our country. We work every day with the FBI, with the NCTC, in gathering information and sharing data. So in that sense, I think our capacity is much more effective than it was 13 years ago. There is always room for improvement and change, but I think the leadership of the counterterrorism (CT) community of our government understands that if we do not cooperate, bad things will happen.

I think the nature of the threat is—I think Nick probably characterized it best. On September 11, 2001, we were focused on al-Qaeda in Afghanistan and Pakistan. Today al-Qaeda, al-Qaeda adherents, and other jihadists are essentially global. They are operating in North Africa. They are operating in the Middle East. They are operating in South Asia. So much more diverse. Nonetheless, they still see us as the enemy and, therefore, a threat to the United States and our operations around the world.

Senator JOHNSON. Mr. Rasmussen, I believe the threat is growing. I think it is more grave. You had mentioned the effect of Edward Snowden's disclosures. Has that degraded our ability to protect ourselves? Has that degraded our intelligence-gathering capabilities?

Mr. RASMUSSEN. I would argue yes. I can talk in greater detail in a closed session about some of the specific information or indicators we have seen that would lead me to that conclusion. But I think it is inarguable that the collection environment we are in—and we rely on collection to be able to try to get ahead of terrorist plots. It is inarguable that that collection environment is more challenging today than it was if we had not been dealing with these disclosures.

Senator JOHNSON. In a Foreign Relations Committee hearing, we had Deputy Assistant Secretary of State Brett McGurk, and I asked him directly: What threat does ISIS directly pose to the United States? He talked about the 30 to 50 suicide bombers funeling into Iraq that week. We had an Australian and a German suicide bomber set themselves off, I believe in Baghdad. We have seen the first American suicide bomber. I am concerned, the talk coming out of this Administration that this may take 3 years.

First, let me ask you: Do you believe ISIS is something that can be contained or managed versus destroyed?

Mr. RASMUSSEN. I think of this in phases. I think in the near term, in the immediate term, you can take steps to degrade and disrupt their ability to carry out attacks. But to prevent yourself from having to deal with that in perpetuity, you have to go beyond that and look to destroy or defeat the organization, and that is what the Administration, the President, and the Secretary of State have talked about over a long period of time. That objective is not as easy to put a specific time horizon to.

Senator JOHNSON. I understand, but I am concerned, kind of like having a hornet's nest in your backyard. You identify the threat; you want to get rid of it as quickly as possible. You do not want to poke it with a stick for 3 years. So, again, what I want to see is a clearly articulated goal of destroying ISIS as quickly as possible so that we can then maintain our defenses against the other threats that are metastasizing around the world. Would you basically agree with that assessment?

Mr. RASMUSSEN. I certainly share that goal. I think the talk about the phasing is just simply a recognition that in order to build the intelligence basis necessary to attack and pull apart an organization and defeat it takes time.

Senator JOHNSON. OK. I understand.

Mr. RASMUSSEN. But while you are doing that, you try to put great pressure on the organization so that it cannot punch you in the process while you are going through that longer process.

Senator JOHNSON. I think one thing we always have to guard against is always fighting the last war, only concentrating on past threats. To what extent is the intelligence community using our imagination in terms of looking at what other possibilities just might be out there?

Mr. RASMUSSEN. We certainly are devoting time and attention to that. Again, pressures of the day often lead you to focus on what

is the wolf closest to the door. And yet we also challenge our analysts and our intelligence community partners to look around the corner and see not only where the next groups might come from, where the next theaters of concern might be, but also what tactics and techniques and opportunities for innovation might exist in the terrorism community as well. That is harder and you are not often relying on much intelligence in that setting. You are often, as you say, using your imagination. But it is important work, and it helps us over time to target our collection to try to get ahead of those particular threats.

Cyber is one of those areas where we have not seen terrorists necessarily develop great capability to date, but they certainly understand the economic impact that intervention in the cyber world causes. And so we assess that over time that is a capability terrorist groups—

Senator JOHNSON. I want to cover that and explore that in the secured briefing a little bit.

Secretary Spaulding, you talked about critical infrastructure. You talked about what our physical and cyber threats are. I want to talk about something that I have been now briefed on, the threat of Electro Magnetic Pulse (EMP), both in terms of a high-altitude nuclear blast, which is kind of what I always knew existed out there, and I guess kind of hoping that nobody has the capability or would not be stupid enough to do it, but now also aware of the fact that a massive solar flare also represents a real threat. That is something that you are certainly aware of. Is that something we are looking to harden our electrical grid against?

Ms. SPAULDING. Absolutely, Senator, and thank you for the question. It is certainly something that we have been focused on and working with our colleagues in the electric sector to find ways to address.

I was recently in the U.K. at an international conference, an energy infrastructure security summit, where EMPs were a clear focus of those discussions. This is something very much on our radar screen and that we are working with them to address.

Senator JOHNSON. OK. We will cover more of that. Just real quick, in terms of the—for Mr. Anderson, the attack at the Metcalf Pacific Gas and Electric (PG&E) substation, do we have any further information you can share in open session in terms of have we tracked down the perpetrators, have we come up with theories in terms of what that was all about?

Mr. ANDERSON. We are heavily engaged in that investigation, Senator, and it would be easier to describe to you everything that we are doing inside the closed session.

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

Chairman CARPER. Thank you. Senator McCain.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Thank you, Mr. Chairman, and I thank the witnesses.

Mr. Taylor or Mr. Rasmussen, haven't there been recent reports on Twitter and Facebook of messages that would urge infiltration into the United States across our Southwestern border?

General TAYLOR. Yes, sir, there have been Twitter social media exchanges among ISIL adherents across the globe speaking about that as a possibility.

Senator MCCAIN. Would you view it as a threat?

General TAYLOR. Certainly any infiltration across our border would be a threat, but in the course of our border security——

Senator MCCAIN. Are you satisfied that we have sufficient border security to prevent that?

General TAYLOR. Sir, I am satisfied that we are trying to build a border security capability that would address that——

Senator MCCAIN. Are you satisfied that we now have the capability to prevent that?

General TAYLOR. I am satisfied that we have the intelligence and the capability at our border that would prevent that activity.

Senator MCCAIN. Well, it is interesting, because an American reporter named James O'Keefe dressed as Osama bin Laden walked across the border, the Rio Grande River, undetected. Does something like that concern you?

General TAYLOR. Actually, sir, he was not undetected. He was known to the border security agencies who saw him walk across.

Senator MCCAIN. Then why didn't they stop him when he came across?

General TAYLOR. Sir, I cannot answer that question——

Senator MCCAIN. No, you cannot answer it because they were not there to stop him, and that is a matter of being on record.

The fact is that there are thousands of people who are coming across our border who are undetected, who are not identified. And for you to sit there and tell me that we have the capability or now have the proper protections of our Southwestern border, particularly in light of the urgings over Facebook and Twitter for people to come across our Southwestern border, is of great concern to the citizens of my State. I would like to hear your response to that.

General TAYLOR. Sir, the security at the Southwest border is of great concern to the Department, and certainly I understand the concerns of the citizens of your State. If I gave you the impression that I thought the border security was what it needed to be to protect against all the risks coming across the State, that is not what I intended to say.

Senator MCCAIN. Could you give to the Committee for the record what is required to achieve 90 percent effectiveness control of the border and prevent this threat from materializing? Because I do not think there is any doubt—I do not see when you look at ISIS and the growth and the influence of ISIS that it would be logical, as they are saying on Facebook and Twitter, to come across our Southwest border, because they can get across. And the flow of drugs across our Southwest border has not been decreased by any significant measure. Would you agree to that?

General TAYLOR. The flow of drugs continues to be significant, yes, sir.

Senator MCCAIN. Well, those of us who strongly supported comprehensive immigration reform are deeply disappointed in our lack of devotion of assets and funds and capabilities to secure our Southwestern border, which has then created a credibility problem in our States and across this country that we can guarantee people,

if we enacted comprehensive immigration reform, that there would not be another flow of refugees or illegal immigration into this country. Now we have this phenomenon or, I guess, occurrence of thousands of young children showing up at our border, not trying to sneak across but just showing up at our border. It has tailed off some, but it is still by the thousands. And isn't this diverting the assets and the capabilities of our Border Patrol by having to handle this incredible influx of children, diverting them from other duties like trying to interdict drug smugglers and others? And isn't it true, could I say to you—and it is really astonishing to me how our friends on the left and those who are “pro-immigration” ignore the fact that the brutalities that are inflicted on these young people, particularly young women, as they are brought across by these coyotes is absolutely abhorrent and unspeakable. Would you agree with that?

General TAYLOR. Absolutely, Senator, I would agree with it. And to your earlier question, we not only assess, we believe the Border Patrol has done an absolutely remarkable job in handling the unaccompanied alien children (UAC) crisis, and——

Senator MCCAIN. But they have been diverted, right?

General TAYLOR. It has been a priority, given the number of people at our border, to focus on that issue, and certainly with the resources as they are, resources are shifted to priorities.

Senator MCCAIN. So it has always been a national security issue, but I believe that in light of the growth of ISIS and the aggressiveness of ISIS and the information that they have been able to recruit in the United States of America—we know that because Americans have been killed over there—that it seems to me it dramatically heightens our requirement to have a secure Southern and Northern border. Would you agree with that?

General TAYLOR. I absolutely agree with it, Senator.

Senator MCCAIN. Thank you. And finally, Mr. Rasmussen, it is entertaining to me that it is like it all just happened with ISIS, another wolf at the door. We have known about ISIS for 4 years. People like me and Lindsey Graham and many others have known about it and warned about it and talked about it, while we have done nothing to really stem the tide and the growth of ISIS and the chaos that we now see pervading Iraq and Syria. Some of us are hopeful that the President of the United States will finally recognize that threat and outline to the American people some actions that need to be taken. But many of us predicted this, many saw it coming, and it comes as no surprise.

I thank you, Mr. Chairman.

Chairman CARPER. You are welcome. We thank you as well.

Senator Baldwin, and then Senator Portman, and Senator Ayotte. Senator Baldwin.

OPENING STATEMENT OF SENATOR BALDWIN

Senator BALDWIN. Thank you, Mr. Chairman.

Mr. Taylor and Mr. Rasmussen, I want to talk a little bit more about the estimated more than 100 U.S. persons who have left to join the fight in Syria. I think that is how it was phrased. And I just want to get a sense of, is this an estimate or do we have a sense of actually who these 100-plus people are, names, where they

are from, et cetera? How much detail do we have? Or are we basically just estimating that it is about 100?

Mr. RASMUSSEN. I will take a stab at that, Senator. That number is actually meant to capture a number of categories of individuals who have shown an intent to travel and that travel has not happened, individuals who have traveled, individuals who have traveled and come back, individuals who have traveled and perhaps been killed in the fighting over there. And so that number is somewhat all encompassing and does not necessarily reflect an estimate of who is exactly there right now today.

There is more we can say with greater precision in the closed session, but I think I can reassure you there is some significant detail behind that broad number.

Senator BALDWIN. Great. I am going to try to ask a couple more questions in open session on this topic. We will see how far we can get.

With regard to that number, is there differentiation, very specific differentiation, between those who are actually joining ISIL and those, for example—I traveled to Turkey now over a year ago, but there were certainly American citizens of Syrian descent who were there trying to provide humanitarian relief in the fight or trying to do what they could to help the moderate rebels, the moderate elements, try to participate in battle there. Are we differentiating between those when we talk about these rough numbers?

Mr. RASMUSSEN. Yes, we are. As I said, we are——

Senator BALDWIN. OK.

Mr. RASMUSSEN. And in some cases, we know of individuals who have indicated intent or have traveled to Syria who go over not necessarily knowing who they will affiliate with when they get there. They simply look to join the fight from an extremist or jihadist perspective, and where they actually end up affiliating plays out over time, and we may or may not have intelligence on that. But you are right, the number of individuals who have traveled to Syria can capture people who engage in a wide variety of activities there.

Senator BALDWIN. But that 100 or whatever we are tossing around, over 100, you believe are engaged in the battle with the ISIL extremists?

Mr. RASMUSSEN. With extremist elements. I want to be careful and not pin it——

Senator BALDWIN. I understand.

Mr. RASMUSSEN [continuing]. Strictly to ISIL because, as you know, there are a number of organizations——

Senator BALDWIN. Right.

Mr. RASMUSSEN [continuing]. Over there, al-Nusra Front——

Senator BALDWIN. And I am getting there, too. Before I get to that second point, do we have a sense that, in particular, our European allies have as granular information on their citizens who have traveled to Syria as we do on ours?

Mr. RASMUSSEN. I think it is not a constant picture across the whole of Europe. I think in some cases, with some of our partners with whom we work the most closely, the answer is absolutely yes. They have a very detailed understanding of individuals, and, in fact, they have done a great deal of work talking to in many cases

individuals who have come back from Syria in order to try to understand both the appeal and the draw, but also the experiences those individuals had and how they may play—what contribution to the threat picture back in their homes that they may present. And I know that a significant amount of law enforcement effort in the United Kingdom, for example, is devoted to just that effort.

But I would not argue that this is constant across the whole of Europe. In many of the particularly Southern and Eastern European partners which are closer to the front line of travel to Turkey and Syria, their capabilities just simply are not as well developed, they are not as well resourced to handle a large national security challenge like this in the way that some of our more traditional partners are.

But as I pointed out in my statement, there is a bit of a good-news story in that the willingness to at least lock arms with us and share information is something we have seen pretty constantly across the board.

Chairman CARPER. Senator Baldwin, just to interrupt for a second, Senator Coburn as a member of the Intel Committee just shared with me a cautionary note. You will have a good feeling for what is appropriate to say in an open setting and what is more appropriate to say in a closed setting, again, if you ask questions that you think should be deferred to the next part of our hearing, please do that. Go right ahead.

Senator BALDWIN. So do we have a sense of how many U.S. nationals are engaged with al-Qaeda globally, and obviously there is a much greater fragmentation and even in particular al-Qaeda in the Arabian Peninsula? Do we have that same sort of granular information there?

Mr. RASMUSSEN. Again, I think it varies depending on which al-Qaeda affiliate group you are talking about, and we can certainly talk about specific cases involving specific known individuals in another setting.

Senator BALDWIN. OK. And then can you describe in open session for the Committee what we know, what our intelligence has said about the relationship between ISIL and al-Qaeda? Is it a rivalry? Is it cooperative? Are they rooting each other on? What do we know at this point about their relationship?

Mr. RASMUSSEN. Well, one of the things that I think has been a development that we have spent a great deal of time trying to understand and assess is the degree of conflict intention between ISIL and Core al-Qaeda leadership, as I said, resident in the Fatah. And I think what you could argue now you are seeing, in a sense, a contest or a competition for primacy in that overall effort to lead the global jihad, with ISIL increasingly posturing itself as the legitimate follow-on or heir to Osama bin Laden and the al-Qaeda vision. And what that is also doing is causing, I would argue, intellectual ferment in that broader jihadist community around the world—we see this in other al-Qaeda affiliates—as they seek to decide for themselves, Do we align with ISIL or do we maintain fidelity to our traditional bonds of loyalty to al-Qaeda Core?

I think one thing we can observe pretty obviously is that success breeds success, and so that when ISIL has had success on the battlefield in taking over large swaths of territory in Iraq, that has

served as a draw not only to foreign fighters who might want to choose where to bring their capabilities, but also to individuals who may be affiliated with other al-Qaeda groups who decide, "I would like to go where the jihad is the most hot and where my ability to impact global jihad can be felt most acutely." And there is no doubt that at the level of individual al-Qaeda-affiliated individuals, that draw is out there. And it is something that we will see that will play out over time, whether ISIL would supplant al-Qaeda Core in terms of overall leadership of the global jihad. But it is clear if things trended in this direction for a long period of time, one could make that argument.

Senator BALDWIN. Thank you.

Chairman CARPER. All right. Thank you, Senator Baldwin.

Senator Portman, please.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Mr. Chairman, and I appreciate the testimony today and the opportunity to ask followup questions in another session.

There is so much to go over, but I want to talk a little about what you have said today and what some of my colleagues have asked about in terms of Iraq and ISIL and how we got in this situation that we are in. Because I think it is important not only to determine what we do now in Iraq but also to look to Afghanistan and what we are doing or not doing there to ensure that we do not have a similar situation.

With regard to Afghanistan, how do you assess the security forces there, the Afghan security forces, as compared to the Iraqi security forces, Mr. Rasmussen?

Mr. RASMUSSEN. I would want to come back—

Senator PORTMAN. Specifically their capability to conduct counterterrorism operations against the Taliban and al-Qaeda partners.

Mr. RASMUSSEN. I believe we have made a substantial amount of progress in bringing the Afghan National Security Force up to the level where they can carry out counterterrorist operations against known terrorist targets inside Afghanistan. What we will not know until we see over time is whether the Afghan Government is able to sustain that capability, invest and resource and sustain that capability over time so that they are able to do this as they encounter threats—

Senator PORTMAN. Do you think they have greater capabilities than the Iraqi security forces, assuming that, as was the case over the last few years, there is no U.S. support?

Mr. RASMUSSEN. I am reluctant to put it in comparative terms because I am not sure I have the right expertise or knowledge to do that, and I would be happy to get you an answer to that from—

Senator PORTMAN. I think it would be interesting. I mean, here is my feeling from some of your reports which were made public and other assessments, is that, in fact, the Iraqi security forces were further along at the time at which we chose to pull out. And if we decide to do the same thing in Afghanistan and that the President has said that he has plans to have no more troops in Af-

ghanistan by the end of 2016, that we may have a similar and I would say worse situation given the assessment of their capability to be able to have an effective counterterrorism operation.

So I would just make the obvious point that we need your help in terms of learning lessons from Iraq and hopefully taking those lessons to Afghanistan.

There has been a lot of attention recently to President Obama's comments last January about regional terrorist groups being like JV teams in relation to ISIL's seizing of Fallujah. I am sure you have followed that back and forth. And, Mr. Taylor, General Taylor, and Mr. Rasmussen, I am not going to ask you if you shared that assessment at the time because the President indicated that was an assessment that he had. But I will say, given all the bloodshed and resources expended in the two attempts to take Fallujah in 2004—and I was privileged to go there at one point in the 2004–05 time period, and those years of toil by our marines and soldiers in Anbar that followed to make it a peaceful place, those comments are particularly disconcerting. As you all know, we took serious losses. In one 6-month period in 2005, Ohio's reserve marine infantry battalion lost 46 marines; 22 were killed from one rifle company in Columbus. So obviously the struggle affects a lot of our communities, including back home in Ohio.

I would ask you, Mr. Rasmussen, in 2013, did the intelligence community identify that al-Qaeda-associated groups in Syria had expressed interest in external operations?

Mr. RASMUSSEN. Yes, and we can talk about that more in closed session.

Senator PORTMAN. OK.

Mr. RASMUSSEN. But yes.

Senator PORTMAN. In 2013, did the intelligence community assess that a threat existed to Western Europe and the homeland from the flow of foreign fighters to and from Syria and Iraq?

Mr. RASMUSSEN. Absolutely.

Senator PORTMAN. Do you assess that the Iraqi security forces who earlier this year had been operating without U.S. troops by their side for 2 years took any successful actions to wrest control of Fallujah from ISIL after they seized it in January 2014, earlier this year?

Mr. RASMUSSEN. I would like to get an answer for the record for you on that, because I am certainly aware of Iraqi security force counterterrorism actions, but I want to be specifically responsive—

Senator PORTMAN. Well, let me ask a more general question. Were they successful in wresting control back?

Mr. RASMUSSEN. Not in wresting control back of the areas you describe, as I understand it.

Senator PORTMAN. OK. I just think, again, we should learn some lessons from this. Finally, I would say do you assess that over the last 2 years that ISIL exploited access to fighters and resources in Syria as well as inconsistent counterterrorism operations or pressure from the Iraqis in Iraq to escalate their operations?

Mr. RASMUSSEN. It is certainly true that they have escalated their operations and they have taken advantage of the lack of a real border between Iraq and Syria, which has allowed them to

move resources back and forth to escape counterterrorism pressure, whether it comes from the Iraqi security forces or other elements inside Syria who are fighting.

Senator PORTMAN. Well, I think your answers to these questions are helpful in terms of us understanding what we should be doing in Iraq, but also, again, looking forward to Afghanistan, being sure that we are prepared to take the steps to avoid a repeat of this.

Let me change topics, if I could, and this has to do with the Ebola crisis. General Taylor, I am interested to hear what work your office is doing to monitor the spread of Ebola in Africa. We now have over 2,300 people who have died. The World Health Organization (WHO) tells us today they expect 20,000 people to die relatively soon. There are other groups that have much higher estimates. As you know, we had another U.S. citizen infected this week.

If you could tell me, how are you monitoring this situation in Africa? What are you all doing?

General TAYLOR. Sir, I&A, my office, works with our Office of Health Affairs who is leading the effort of the Department in an interagency response to the Ebola virus and its consequences potentially to the United States as well as in the Africa region. There are daily interagency meetings on that issue and trying to get aid to those countries to stem the spread of the virus, which has been—

Senator PORTMAN. Do you feel we have an effective interagency and intergovernmental coordination?

General TAYLOR. I think we have effective U.S. interagency and intergovernmental coordination, but this is a global problem, and it is going to take a global solution to solve it. And the nations in the region are less capable in certain cases of handling the kind of infection that they are seeing, so it will require a global effort to stem this particular issue.

Senator PORTMAN. General Taylor, I understand Health Affairs is taking the lead here, but have you had the opportunity to look at what the U.S. Government did in relationship to malaria in the Malaria Initiative, the intergovernmental and in that case interagency process that we use?

General TAYLOR. I have not personally looked at it, sir. I am just only aware of the efforts. My most recent experience has been with H1N1, which I think we had a very effective interagency coordination on that, but not the malaria.

Senator PORTMAN. I am concerned that we are, again, not being as aggressive as we could be, and I would just hope that the agency would take a look at what we have done in the past, and we have been relatively successful, not just with AIDS but also with the specific steps that we are taking on the Malaria Initiative to try to get more countries engaged and deal with the issue.

One final question. Do you have any insights on how you see the spread of Ebola developing and what we should be doing here in this country? I noticed that, Ms. Spaulding, you talked about the National Preparedness Month, and one of my concerns is, based on some recent reports, we are not prepared. We have, unfortunately, a situation where if a pandemic were to occur, there are some

shortfalls, including expirations on some of the medical response that will be necessary. Do you have thoughts about that?

General TAYLOR. Sir, I would prefer to respond in a more holistic way in consultation with my colleagues, so if I could take that—

Senator PORTMAN. We would appreciate you getting back to the Committee on that.

General TAYLOR. Yes, sir.

Senator PORTMAN. Thank you. Thank you, Mr. Chairman.

Chairman CARPER. Thank you. Thanks for those questions, especially the last one. Senator Ayotte, after you have spoken, asked questions, I am going to give Mr. Anderson an opportunity—we have not picked on you enough. I will just give you one opportunity for any point that you want to make or share with us in the open session before we go to the closed session. You will have that opportunity, OK?

For now, Senator Ayotte.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. Thank you, Mr. Chairman. I want to thank you for holding this important hearing. I want to thank our witnesses for what they do to keep the country safe.

Secretary Taylor, I wanted to followup on some of the questions that Senator Baldwin had asked, and I would ask all of you to give me some insight on a comment that I heard from our FBI Director. I think it is important that the American people understand what we are dealing with in terms of not only Americans but Westerners who have potentially traveled to Syria or have interest in traveling to Syria and joining with one of these extremist groups, including ISIL.

So you had testified that more than 100 U.S. persons you are tracking, and you have identified those as those who have intended to go, those who have gone, and some of whom have been actually engaged and killed in this conflict.

I note that the FBI Director Comey said in August, “When I give you the number of 100 Americans, I cannot tell you with high confidence that it is 100 or 200, that it is 100 or 500, that it is 100 or 1,000 more, because it is so hard to track.” Here is a very important question that I think people need to know, and that is, do we really know? And how many of these do we really have track of? And how many don’t we have track of?

General TAYLOR. Senator, I would share Director Comey’s comments in terms of we do not know what we do not know, and I think that is the context in which he was making those comments. I think we have very high confidence on the number that we do know, and we have systems that help us identify more day in and day out. So I could sit here today and give the number of over 100, and tomorrow it may be that, based upon our intelligence investigation with the FBI, we would have more identities that we did not know about before.

Senator AYOTTE. But is the reality that while we have confidence in the 100, we really do not know how many more may be part of this?

General TAYLOR. I think that is a fair statement.

Senator AYOTTE. I assume that is why Director Comey, who I certainly have a lot of respect for, made that statement when he was specifically asked about how confident we are in the number of 100.

General TAYLOR. Well, given homegrown violent extremism, given the nature of how people radicalize, given the nature of the data on the Internet, it is very difficult to say with any degree of certainty that we know all that could be wanting to join this particular effort.

Senator AYOTTE. So we know that it may be more than the 100 that we are talking about. With respect to the 100 that we do know, do we have track of all of them?

General TAYLOR. Yes, ma'am, I would defer to my colleagues at the FBI who lead the joint task force looking at this issue for our government.

Mr. ANDERSON. Senator, if I could address that, so I agree with General Taylor wholeheartedly. I could tell you any individual—and they definitely fit into the three categories that Mr. Rasmussen had talked about. Any individual that we can predicate an investigation on, the FBI has an open case on that individual, whether they are abroad or in the United States. We also dedicate an immense amount of resources to covering the individuals that we know about. I cannot actually get into all those in this session, but we will in detail in the next session.

Senator AYOTTE. Let me ask you, the 100 that we know about, what authorities do we have to revoke their passports? In other words, you are a United States citizen. Obviously you are entitled to certain rights. But what can we do to make sure that they cannot get back in the community if we believe that they have joined, for example, an extremist group like ISIL who has brutally and horrifically murdered two American journalists?

General TAYLOR. Senator, it is a very complicated question in terms of taking away an American's passport. There are judicial means to do that. I am not an expert in that, but we can get you the answer of what are the authorities that would allow for that to happen.

Senator AYOTTE. Well, I think that is really important because we need to understand. We certainly do not want a situation where you all talk to someone, you do not have the authority to detain them, we are in a position where they have to appear before a judicial authority, but in the interim they are not detained and they have open access in America. So I would like a followup to know what those processes are, what tools you have at your hands when there is obviously evidence that an American is involved with a group like ISIL so that we can understand whether those authorities are sufficient. So I would appreciate a follow-up on that.

I also wanted to ask, what I understand from hearing your testimony today is that you said that the threat of ISIL is really regionally focused, meaning the region of where they are operating in Iraq and Syria and the surrounding regions. What kind of access do they have to financing?

Mr. RASMUSSEN. That has been one of our great concerns as ISIL has surged in Iraq, is that they have had the ability to draw on

a wider array of sources for financing, including kidnap for ransom, simply occupying and taking over Federal Reserve holdings——

Senator AYOTTE. I saw an estimate of they are making at least \$1 million a day. Is that a fair statement?

Mr. RASMUSSEN. That is a fair estimate.

Senator AYOTTE. OK. And as I understand, they have safe havens in Syria, correct?

Mr. RASMUSSEN. Yes.

Senator AYOTTE. And they are obviously taking over more territory in Iraq, correct? That is their design and one of the concerns we have with regard to what is happening in Iraq right now?

Mr. RASMUSSEN. That is their ambition. In Iraq in recent weeks, Iraqi security force action in combination with United States military action has stemmed the ability of ISIL to gain more territory.

Senator AYOTTE. But they have some territory right now, you would agree with me.

Mr. RASMUSSEN. Yes.

Senator AYOTTE. They have territory in Syria; they have territory in Iraq. They have a means to make money. And when we think about this threat on the passport issue, it is not just about Americans, right? I know, Secretary Taylor, in your testimony there are about 2,000 Westerners, but I have also seen estimates of 7,500 potential foreign fighters from all different countries that have joined this conflict, starting in Syria. I do not know how many of those have joined ISIL, but this threat goes beyond thinking about Americans.

I know you talked about a good news story about more communication between other countries with regard to these individuals who have joined these extremist groups. But we also have a visa waiver program with countries like the United Kingdom and France, and so how good is our intelligence and ability to track those individuals? We talked about the 100, so we are worried about our people. But thinking about the individuals that do not need a visa to come travel to the United States of America, and as I understand it, there are actually thousands—the numbers that Great Britain is facing is much greater even than the United States. Can you give us a good assessment of how good a track we have on them and what ability we have to stop them from coming to the United States or to know exactly where they are so that we do not face a situation where someone is—the James Foley video, that individual who committed that barbaric murder, he was clearly from Great Britain. You could tell from his accent. So an individual like that coming to the United States and then participating in an action here.

So can you give us a little more insight on that? Because I think it is important for people to understand.

General TAYLOR. Yes, ma'am. I would defer to Nick to talk about the intelligence cooperation that we have, which is significant, with our European partners and daily we exchange information. More importantly, a visa waiver does not mean people come to this country without screening. Every passenger coming to the United States from outside the United States is screened through our terrorist screening system, and if there is derogatory data, they are not allowed to come to the United States. So——

Senator AYOTTE. But that assumes we have the data, correct?

General TAYLOR. Well, that assumes we have the data, and that is what intelligence collaboration and cooperation is all about, is making sure that, with our partners in Europe and other places, we are getting that data and getting it in a consistent fashion.

Senator AYOTTE. So I think this is all obviously a very important issue as well as knowing and tracking who these individuals are, if we do not have the data, we may just allow them in our country without being able to stop them from coming.

My time is up, but I just want to say one thing that concerns me. I know we have talked today about believing that the focus on the threat of ISIL is a regional threat, but here we have a sophisticated terrorist organization which our own Secretary of Defense has said is beyond anything that we have seen. And, in fact, we have a situation where, Secretary Dempsey described this group as “an imminent threat,” and combined with the fact that they have financial means to make money. They have territory and some safe havens. We know that in January their leader basically threatened the United States of America. We have seen through their actions with the brutal murders of these two journalists that obviously the threat that they face—the type of barbaric actions they are willing to take against Americans. And then we know that if these people who join this, if we are not quite sure how many there are and who could return to the United States. I am concerned that it is an understatement to say that this is a regional threat in terms of what it might present to us in our homeland.

Mr. RASMUSSEN. Mr. Chairman, can I respond to just one—

Chairman CARPER. Yes, just briefly.

Mr. RASMUSSEN. By using the word “regional” in my remarks at the beginning, I by no means meant to imply not directed at the United States or U.S. citizens, because certainly today, currently, ISIL has the capability to threaten U.S. persons and interests not just in Iraq proper but in surrounding regional States. So our embassies, our personnel, our diplomats, and even non-official Americans are certainly—

Senator AYOTTE. But what about here?

Mr. RASMUSSEN. As I said, if allowed over time to utilize the safe haven that they currently are enjoying—

Senator AYOTTE. So right now you do not think they have that capacity.

Mr. RASMUSSEN. Right now we assess that they do not have active, ongoing plots aimed at the United States homeland.

Senator AYOTTE. So that is a different question of whether they have the capacity. We do not know of any active, ongoing threats or plots, but—

Mr. RASMUSSEN. And we do not assess right now that they have the capability to mount an effective, large-scale plot inside the United States.

Senator AYOTTE. Large scale, correct?

Mr. RASMUSSEN. Another piece of this that you cannot necessarily account for are individuals that we talked about under the category of homegrown violent extremists who may self-identify as acting in sympathy with or in support of ISIL, maybe perhaps not even ever having touched ISIL leadership in any kind of command

and control way, but in the aftermath of a potential attack, even here in the homeland, might self-affiliate and describe—so I do not mean by any means to minimize the threat to ISIL. That is not my intent. I was simply trying to describe in, kind of in a sense, concentric rings the levels of concern that we have at present versus what we see developing more over time.

Senator AYOTTE. Thank you.

Mr. RASMUSSEN. There is no doubt that what you have described with the foreign fighters is what gives them the capability to threaten the homeland over the longer term.

Senator AYOTTE. OK. Thank you.

Senator COBURN. I would just add one point. You have to take, in fact, the exhortation of various members of ISIL to come across our Southern border. It is out there. It is in the social media. So I know you all are looking at that, but the fact is that is pretty scary because you talk about what we do not know. We do not know the people who are coming across our border, what their threat is to us. We do not know.

Chairman CARPER. I said, Mr. Anderson, we would give you an opportunity to have a closing thought, please.

Mr. ANDERSON. Thank you, Mr. Chairman. If I could, I would just make a closing remark and turn back to cyber for a second.

The one thing that I think the Committee needs to know—and they probably do—is when it comes to cyber, I have never seen more cooperation in my entire law enforcement career than I have in the last year or so. The people at this table, DHS, Secret Service, a large variety of our intelligence partners, we all get it. We get that this is something that is going to go through from now to the next several years in our government. This is a deep concern of ours, to work together and work toward a fix.

When we talked a little while ago about a number of Federal departments within our government possibly could be hacked, or if they were hacked and they just did not know about it. I think one of the things that I know we are all working on and I know the legislature up here is also, we are trying to figure out how we share real-time information with our private sector partners. I think that is absolutely imperative, Mr. Chairman, and I think my colleagues here would echo that. And one of the main reasons is because everyone knows a lot of our classified and very sensitive technologies are developed, designed, and then built out in the private sector way before they are ever classified. Our adversaries know this, whether it is counterintelligence, counterespionage, economic espionage, counterterrorism. I have had the pleasure over the years to testify as the Assistant Director of Counterintelligence to Chairman Feinstein, also Dr. Coburn many times regarding this kind of scare for us. And I would tell you that the one thing that I see is the whole of government coming together as one on this threat and really working toward a positive fix.

Thank you, Mr. Chairman.

Chairman CARPER. And I would just add to that, the threat of ISIS and these other terrorist groups, are they a threat? Sure they are, and we have to be eternally vigilant. And this is not any time to pat ourselves on the back and become complacent. If anything, it is time to be more vigilant. We will see what the President has

to say tonight. I hope he will be very strong. I hope he will lay out a game plan that will enable us, working with an armada of other nations around the world, to destroy this threat. And that is what I am looking for, and hopefully that is what we will get.

I would also say just one last word. I always come back to underlying causes, root causes. And, Nick, when I visited, we talked about underlying and root causes. And I would just say a couple of them.

One underlying cause, al-Qaeda in Iraq was on their back, they were almost done about 7 years ago. And the policies of the Iraqi Government actually helped them get off the mat and back into the game and to be the threat that they are today. And my hope is that the new prime minister, the new government that is being stood up in Iraq will be part of the solution to help us accomplish what we did 7 years ago and to do it again, and only this time for good.

All right. You have been great to be here with us. I appreciate our colleagues being here as well. We are going to move to a secured setting, and with that, this portion of the hearing is adjourned.

[Whereupon, at 11:16 a.m., the Committee proceeded to other business.]

A P P E N D I X

**Opening Statement of Chairman Thomas R. Carper:
“Cybersecurity, Terrorism, and Beyond:
Addressing Evolving Threats to the Homeland”
September 10, 2014**

As prepared for delivery:

Almost every year, this committee holds a hearing to review a multitude of threats to our homeland and examine how our government is working to counter them. We routinely hear from the Department of Homeland Security, the FBI and the National Counter Terrorism Center about how we can best keep Americans safe from those who seek to carry out deadly attacks against our country and its people. We also hear about actors in cyberspace that want to drain our bank accounts, shut down our financial system and our electric grid, steal our individually identifiable information and our identities, as well as the R & D that will enable American businesses and our military to remain pre-eminent in the world.

Assessing these ever-changing, broad threats and making sure our government continues to hone its ability to stop them remains a top priority for this committee, particularly as we approach another 9/11 anniversary. This year, our hearing takes on an added significance, as our nation confronts a growing terrorist threat in Iraq and Syria. As we sit here today, our military is engaging in limited airstrikes in Iraq in an effort to dislodge and repel that threat. Later this evening, President Obama will address our nation. He is expected to share with us and the world the steps that he is recommending be taken in Iraq and in Syria to reverse the expansion of the Islamic State of Iraq and Syria and enable the people who live in those countries to reclaim their lives.

Much of the world has been exposed to a steady stream of deeply disturbing images from that region in recent weeks. Brutal executions. Human rights atrocities. Repression of women. And a seemingly endless procession of masked militants defiantly waving the black flag of jihad in celebration of their brutality. Effectively addressing the threat from the newly-proclaimed Islamic State of Iraq and Syria will require a multifaceted strategy. That strategy will need a military component and the development of a robust international coalition to execute it. Among the goals of that strategy is to ensure that the Islamic State of Iraq and Syria does not establish a long-term safe haven from which it can launch attacks against either our allies or our homeland – much like we saw with al Qaeda in the days before 9/11.

Today, we will examine the steps that our federal government has already taken, along with the steps we still need to take, to prevent this from happening. We will drill down on this threat and its impact on our homeland, both in this open hearing as well as in a classified briefing directly following. That's not all we're going to do, though. In addition to examining the more conventional terrorist threat the instability in Iraq and Syria may pose, we will also closely examine another major threat that affects our homeland daily: cyber attacks.

Every day, nation states and their affiliates, criminals, terrorists, and hackers launch cyber attacks against our government agencies, our businesses, and important parts of our daily lives such as utilities and financial networks. Some of these actors want to steal our sensitive information to sell it on the black market or to gain a competitive edge. Others are trying to make a political point. Some, however, would like to use a cyber attack to cause wide-scale economic damage or even physical harm. Many of them are good at it, and they're getting even better. We need to stay a step ahead of them. Today, we'll hear in the open portion of this hearing and also in the closed portion how we plan to do that, not unlike the steps we've taken to address terror threats in the wake of 9/11.

Congress clearly has a role to play here. Actually, several roles. One of them is an oversight role. It's one that we take very seriously. Another is a legislative role that involves developing legislation to help enable America to anticipate and repel the cyber attacks that we face on an almost 24/7 basis today. In the last several months, this Committee has completed action and reported three separate cyber bills unanimously to the full Senate. One bill would significantly enhance the capabilities of the Department of Homeland Security's cyber workforce. Another would better protect federal agencies from cyber attack. And, a third would codify the cyber center that the Department uses to monitor and respond to attacks to strengthen its ability to do so.

Yesterday, in an op-ed in "The Hill" newspaper, Secretary Johnson recognized the bipartisan efforts of this Committee and talked about the critical need to pass cyber legislation this Congress – I couldn't agree more. In closing, as we mark the anniversary of 9/11 tomorrow, we must keep in mind one of the key lessons we learned since that fateful day thirteen years ago—the threat is always evolving. Not that long ago, crooks used to have to rob a bank to steal our money. Now, they can click a button on a distant computer and accomplish the same goal. Nation states and rival businesses used to employ corporate insiders or retirees to steal company secrets. Now, they send a spear-phishing email. And terrorists used to be a distant threat in the mountains of Afghanistan or Pakistan. Now, an increasing number of them are homegrown. They may be using European, or even, American passports.

So as the threats become more sophisticated, more elusive, and more diffuse, we need to remain ever vigilant to ensure that our government is nimble enough to keep up with tomorrow's threats as they confront us. We have come a long way since 9/11. In many respects, we are more secure than we were on this day thirteen years ago, but the world in which we live remains a dangerous place, so there is always more work to do. When it comes to securing the homeland and anticipating the next threat, we owe it to the American people to strive for perfection. The consequences of failure are simply too high, and the costs too severe.

I'm pleased that we have with us today a panel of witnesses who work together every day to tackle the terrorist and cyber threats we face. Let me express my gratitude to each of you for your testimony and also thank you for your service to our country.

Opening Statement of Ranking Member Tom Coburn**“Cybersecurity, Terrorism, and Beyond:
Addressing Evolving Threats to the Homeland”
Sept. 10, 2014**

As prepared for delivery:

Good morning, and thank you to each of our witnesses today for their testimony. I also want to thank you for what you do, your vigilance, and the criticism you take — much of which is uninformed and undeserved.

Although I agree with Senator Carper’s opening comments in many respects, where I would disagree is I do not think we are any safer today. We have a long ways to go. Based on what is happening in the world and the absolute lack of control of our border—including corruption of law enforcement along our southern border—I think the threats to and vulnerabilities of our country are just as great as they were on September 10, 2001.

The Department of Homeland Security in particular has many problems. But I know the Department has the dedicated leaders it needs now, all concentrating on the same goal of making us safer. So I am glad Secretary Johnson is there, along with General Taylor, Under Secretary Spaulding, and all the others we have confirmed through the Committee.

One of the biggest threats we face is in cybersecurity, where we have seen significant breaches both in the federal government and in the private sector. Most of them are from nation-state actors—China and Russia, specifically. And they will continue to attack us. We should not fall back from talking about what these countries are doing and why they are trying to steal our information and damage our economy. That will require all of us to work together in the cyber-realm to ensure that we reduce our vulnerability.

An important step in reducing our cybersecurity vulnerability is creating true cybersecurity information sharing between the federal government and the U.S. critical infrastructure, and between private U.S. companies. So I think it is a shame that the Senate Majority Leader will not put the bipartisan Feinstein-Chambliss cybersecurity information sharing bill on the floor. Let the Senate debate it, so we can actually start to protect our country from cyber-attacks.

These are real threats. This is an important hearing for the American people to hear—in as much detail as possible—what is going on, the threats we face, and where we need to improve.

Having the privilege of setting on both this Committee and the Select Committee on Intelligence, I get to see as well as anybody what is out there, and what everyone is doing to stop it. And everybody is working in the right direction, except the U.S. Senate. My hope would be that the Senate would start helping to improve homeland security, rather than harm in it.

So, again, I thank you all for your efforts.



Statement for the Record

The Honorable Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate

and

The Honorable Francis X. Taylor
Under Secretary, Office of Intelligence and Analysis
U.S. Department of Homeland Security

Before the
U.S Senate Committee on Homeland Security and Governmental Affairs

Regarding
*Cybersecurity, Terrorism and Beyond:
Addressing Evolving Threats to the Homeland*
September 10, 2014

Introduction

Chairman Carper, Ranking Member Coburn and distinguished members of the committee, thank you for the opportunity to appear before you today to discuss terrorist, cyber and other human-caused threats to the Homeland and the current threat environment on the eve of the anniversary of the September 11, 2001 attacks.

Thirteen years later, we continue to face a dynamic threat environment. Threats to the Homeland are not limited to any one individual, group or ideology and are not defined or contained by borders. They display the increasing determination of individuals to carry out acts of terrorism that have potential to negatively impact the Homeland through loss of life, destruction of critical infrastructure, disruption of technological capabilities or services, or compromise of information security.

In the testimony today, we will highlight some of the threats we face and the risk-informed actions we take that assist government at all levels and owners and operators of critical infrastructure to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools in the four priority areas outlined by Secretary Johnson: (1) aviation security, (2) border security, (3) countering violent extremism, and (4) cybersecurity.

Challenges Ahead

It is important to mention a couple items to provide some strategic context before covering specifics. First, the cornerstone of our mission at DHS has always been, and should continue to be, counterterrorism – that is, protecting the nation against terrorist attacks. We must remain vigilant in detecting and preventing terrorist threats that may seek to penetrate the homeland from the land, sea or air. From a security perspective, many of the resources we expend and activities we conduct apply to both countering terrorism, as well as countering transnational criminal organizations, and other homeland security challenges.

Second, to address the range of challenges the nation faces most collaboratively and effectively within the Department, we have recently undertaken an initiative entitled “Strengthening Departmental Unity of Effort.” In his April 22, 2014 memorandum, Secretary Johnson directed a series of actions to enhance the cohesiveness of the Department, while preserving the professionalism, skill, and dedication of the people within, and the rich history of, the DHS components.

The actions in this initiative: new senior leader forums led by Secretary and the Deputy, and cross-departmental strategy, requirements, and budget development and acquisition processes that are tied to strategic guidance and informed by joint operational plans and joint operations are building and maturing DHS into one that is greater than the sum of its parts – one that operates

much more collaboratively, leverages shared strengths, realizes shared efficiencies, and allows us to further improve our important role as an effective domestic and international partner.

Terrorism and Aviation Security

Core Al Qa'ida, Al-Qa'ida in the Arabian Peninsula (AQAP), and their affiliates remain a major concern for DHS. Despite senior leadership deaths, the group maintains the intent and capability to conduct attacks against U.S. citizens and our facilities, and has demonstrated an ability to adjust its tactics, techniques and procedures for targeting the West in innovative ways. AQAP's three attempted attacks against the U.S. homeland—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot in May 2012—demonstrate their efforts to adapt to security procedures. Over the past several weeks DHS has taken a number of steps to enhance aviation security at overseas airports with direct flights to the United States, and other nations have followed with similar enhancements.

The Islamic State of Iraq and the Levant (ISIL) is a terrorist group operating as if it were a military organization, attempting to govern territory, and their experience and successes on the battlefields of Iraq and Syria have armed them with capabilities most terrorist groups do not possess. The group aspires to overthrow governments in the region and eventually beyond. At present, DHS is unaware of any specific, credible threat to the U.S. Homeland from ISIL. However, violent extremists who support them have demonstrated the intent and capability to target American citizens overseas, and ISIL constitutes an active and serious threat within the region and could attempt attacks on U.S. targets overseas with little-to-no warning. Attacks could also be conducted by supporters acting independently of ISIL direction with little-to-no warning. In January, ISIL's leader publically threatened "direct confrontation" with the United States, which is consistent with the group's media releases during the past several years that have alluded to attacking the United States.

ISIL exhibits a very sophisticated propaganda capability, disseminating high-quality media content on multiple online platforms, including social media, to enhance its appeal. ISIL's English-language messaging and its online supporters have employed—and will almost certainly continue—Twitter "hashtag" campaigns that have gained mainstream media attention and have been able to quickly reach a global audience and encourage acts of violence. Media accounts of the conflict, and propaganda in particular, play a role in inspiring U.S. citizens to travel to Syria. We are aware of a number of U.S. persons who have attempted travel to Syria this year, which underscores their continued interest in partaking in the conflict. More than 100 U.S. persons and over two thousand Westerners have traveled or attempted travel to Syria to participate in the conflict—with some of them seeking to fight with or otherwise support violent extremist groups.

We remain concerned about the threat of U.S. foreign fighters and supporters returning from Syria and whether they would to conduct attacks either on their own initiative or at the direction

of terrorist groups abroad. In addition, a small number of U.S. persons have died while fighting in Syria—including the first suicide bombing by an identified U.S. person in Syria in May and at least one other recently killed while fighting alongside ISIL. These foreign fighters, many in possession of Western passports, have likely become further radicalized while receiving additional training and experience, and pose a potential threat upon their return to their home countries.

The DHS Office of Intelligence and Analysis (I&A) is working closely with interagency partners to evaluate threat data and ensure relevant information reaches DHS personnel and state, local, tribal and territorial (SLTT) partners who can use this information to reduce risks to the Homeland. For example, I&A, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center, produced a poster, handout and muster language for DHS screeners to have background about the conflict in Syria. To ensure our SLTT and private sector partners are kept informed of the current ISIL threat, I&A has hosted multiple calls with our partners in recent months to examine the ongoing situation and, jointly with the FBI, released Joint Intelligence Bulletins (JIB) that provided context and background, examined the potential retaliatory threat and ISIL's use of social media to publicize the group's actions and goals. Following the 9/11 attacks, the importance of an informed community of first responders became clear. I&A places priority on ensuring that the Nation's first responders have the information that they need to identify the trends, tactics and behaviors of a terrorist. It also takes a vigilant public; the Department is dedicated to reminding Americans that "If You See Something, Say Something."

Border Security

Border security must include an intelligence-driven, risk-based approach that focuses resources on the places where our surveillance and intelligence tells us the threats to border security exist, and prepares us to move when the threat moves. The collaborative intelligence work of I&A, the U.S. Coast Guard, the U.S. Customs and Border Protection and the U.S. Immigration and Customs Enforcement helps keep our Southern and Northern borders safe each and every day. We ensure that the officers that are protecting the border points of entry are informed of the necessary intelligence to tailor their operations to the risks poised from overseas.

One of Secretary Johnson's earliest Departmental initiatives was directing development of a Southern Border and Approaches Campaign Planning effort that is putting together a strategic framework to further enhance the security of our southern border. The Plan will contain specific outcomes and quantifiable targets for border security and will address improved information sharing, continued enhancement and integration of sensors, and unified command and control structures as appropriate. The overall planning effort will also include a subset of campaign plans focused on addressing challenges within specific geographic areas, all with the goal of enhancing

our border security. I&A is participating in this effort to ensure threat information drives efficient use of border resources and likewise, that our border analytic focus meets the operational needs of the Department.

Countering Violent Extremism

The individualized nature of the radicalization process for homegrown violent extremists (HVEs) makes it difficult to predict the triggers that will contribute to them attempting acts of violence. Since the Boston Marathon bombings, the Department has evolved to address the need to counter violent extremism (CVE) from an interagency perspective. Mindful of the potential for homegrown violent extremism inspired by radical ideology overseas, we continue to take steps to counter that potential threat, both through law enforcement and community outreach. Beyond the intelligence and information sharing with SLTTs and the private sector, the Department is also committed to training, through the Federal Law Enforcement Training Center, the Federal Emergency Management Agency, the National Protection and Preparedness (NPPD) Office of Infrastructure Protection and I&A. We have a commitment to training to prevent and respond to domestic attacks. Lessons learned from the Boston Marathon bombing highlighted the value in prevention and incident training.

Cybersecurity

Growing cyber threats are an increasing risk to critical infrastructure, our economy and thus, our national security. As a nation, we are faced with pervasive threats from malicious cyber actors. They are motivated by a range of reasons that include espionage, political and ideological beliefs, and financial gain. Certain nation-states pose a significant cyber threat as they aggressively target and seek access to public and private sector computer networks with the goal of stealing and exploiting massive quantities of data.

Some nation-states consistently target Government-related networks for traditional espionage, theft of protected information for financial gain, and other purposes. Increasingly, SLTT networks are experiencing nation-state cyber activity similar to that seen on federal networks. In addition to targeting government networks, there is a growing threat of nation-states targeting and compromising critical infrastructure networks and systems. Such attacks may compromise the infrastructure or control system network and provide persistent access for potential malicious cyber operations which could lead to cascading effects with physical implications.

DHS takes a customer-focused approach to information sharing, in which our desired outcome is to help prevent damaging cybersecurity incidents, such as the theft of personal information or physical disruption of critical infrastructure, and utilizes information in an operational

environment to directly reduce cybersecurity risk. DHS uses information to detect and block cybersecurity attacks on federal civilian agencies and shares information to help critical infrastructure entities in their own protection; to provide information to commercial cybersecurity companies so they can better protect their customers; and to maintain a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information. DHS law enforcement agencies also make substantial contributions to these cyber information sharing efforts.

I&A and NPPD work closely together every day to recognize and reduce risks posed by cyber threats. DHS' National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 operational organization that responds to, and coordinates the national response to, significant cyber incidents. NCCIC is the centralized location where federal departments and agencies, SLTT partners, private sector and international entities all form an operational nexus from which to respond. This centralized location generates collaboration and knowledge dissemination among stakeholders to provide a much greater understanding of cybersecurity vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Supporting the operational cyber mission of NPPD, I&A provides all-source analysis of cyber threats to the '.gov' domain, state and local networks, and critical infrastructure networks and systems to assist owners and operators in protecting their cyber infrastructure. I&A's cyber intelligence products and briefings are tailored to classification levels appropriate for our customers, and include For Official Use Only- and classified-level products and briefings specifically for the state and local audience.

The NCCIC actively collaborates with public and private sector partners every day, including responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks. So far this Fiscal Year, the NCCIC has processed over 612,000 cyber incidents, issued more than 10,000 actionable cyber alerts that were used by recipients to protect their systems, detected more than 55,000 vulnerabilities through scans and assessments, and deployed 78 onsite teams for technical assistance. In one recent example, the United States Secret Service (USSS) shared information on malware observed in recent Point-of-Sale intrusions with the NCCIC for analysis. In partnership with the Financial Services Information Sharing and Analysis Center, the results of this analysis were published and enabled U.S. businesses to identify and stop ongoing cyber intrusions, thereby protecting customer data and mitigating losses.

Cybersecurity Information Sharing

While many sophisticated companies currently share cybersecurity information under existing laws, there is a continued need to increase the volume and speed of cyber threat information sharing between the government and the private sector – and among private sector entities – without sacrificing the trust of the American people or individual privacy, confidentiality, or civil liberties.

The Administration continues to take steps through executive action and public-private initiatives that incentivize and enable information sharing under existing laws. For example, Executive Order 13636 issued by President Obama in February 2013 directed intelligence agencies to increase the speed and quantity of declassified cyber threat information that the government shares with the private sector. Moreover, in February 2014, the Department of Justice and Federal Trade Commission, the two agencies charged with enforcing our antitrust laws, issued guidance that they do not believe “that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing.”

While progress continues under existing law, the Administration has consistently stated that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to improve the Nation's cybersecurity. Accordingly, the Administration continues to emphasize three fundamental priorities for information sharing legislation:

1. Carefully safeguard privacy, confidentiality, and civil liberties;
2. Preserve the long-standing, respective roles and missions of civilian and intelligence agencies. Newly authorized cyber threat information sharing should enter the government through a civilian agency; and,
3. Provide for appropriate sharing with targeted liability protection.

DHS Cybersecurity Authorities

Information sharing is only one element of what is needed. We also need to update laws guiding Federal agency network security; give law enforcement the tools needed to fight crime in the digital age; create a National Data Breach Reporting requirement; and promote the adoption of cybersecurity best practices within critical infrastructure.

We urge Congress to continue efforts to modernize the Federal Information Security Management Act to reflect the existing DHS role in agencies' Federal network information security policies; clarify existing operational responsibilities for DHS in cybersecurity by authorizing the NCCIC; and provide DHS with hiring and other workforce authorities.

These provisions are vital to ensuring the Department has the tools it needs to carry out its mission.

Strengthening the Security and Resilience of Critical Infrastructure

Because the majority of the Nation's infrastructure is owned and operated by the private sector, DHS works with owners and operators, primarily on a voluntary basis, to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools to help mitigate risks. By leveraging its core capabilities, such as information and data sharing, capacity development, vulnerability assessments, and situational awareness, DHS is effectively using its skills and resources to assist with building the Nation's resilience to physical and cybersecurity risks.

DHS works to ensure relevant information on current threats is disseminated as widely and appropriately as possible. Information sharing efforts leverage the existing partnership framework, allowing DHS to discuss threats, protective measures and joint industry/government initiatives with the private sector in order to reduce risk. For instance, DHS and FBI have engaged more than 400 major malls across the United States to facilitate 56 tabletop exercises based on a Westgate Mall, Nairobi-style attack involving coordinated active shooters and use of improvised explosive devices, and requiring a sustained response and deployment of federal resources. In addition, DHS and the Department of Energy, through the Sector Coordinating Council and in collaboration with other interagency partners, provide classified and unclassified threat briefings to CEOs and industry executives on physical and cyber threats. This frequent information sharing allows DHS and DOE to communicate specific threats to the electric sub-sector owners and operators.

The National Infrastructure Coordinating Center (NICC) maintains 24/7 situational awareness and crisis monitoring of critical infrastructure and shares threat information in order to reduce risk, prevent damage, and enable rapid recovery. The NICC makes relevant information available to all critical infrastructure owners and operators through the Homeland Security Information Network, DHS's web-based information sharing platform, bringing together homeland security partners across the spectrum. Finally, the Private Sector Security Clearance Program provides a key support capability to these information sharing efforts, facilitating DHS-sponsored security clearances for critical private sector representatives across the country. This critical ability to share information at the classified level promotes a two-way exchange between the Intelligence and infrastructure protection communities that can directly lead to posturing and protection measures to mitigate risk.

Conclusion

Whether securing the Homeland from aviation threats, border threats, homegrown violent extremists, or cyber threats, DHS has matured over its tenure to recognize that it takes the intelligence, planning, training and operations of our combined components to be effective against all nefarious actors. It is through the great work and collaboration of the DHS Counterterrorism Advisory Board (CTAB) that intelligence and mitigation strategies are synthesized across the Department. The CTAB brings together the intelligence, operational and policy-making elements from across DHS to facilitate a cohesive and coordinated operational response so that DHS can deter and disrupt terrorist operations.

While many of the threats I have highlighted for you today may be emerging and evolving, the Department of Homeland Security has been poised to deal with them and remains ready to respond. Our established relationships and information sharing practices enhance our indications and warning. We continue to work closely with our partners – both here at home, as well as our international partners – to aggressively thwart plans and activities that pose a threat to the homeland. Dealing with evolving risk in a changing world is core to the DHS mission, and is carried out by an outstanding team of professionals across the globe each and every day. We will continue to evaluate and adopt serious and prudent homeland security measures as situations warrant.

Chairman Carper, Ranking Member Coburn and distinguished members of the Committee, thank you for this opportunity to testify about threats to the Homeland. We look forward to answering your questions.

**Hearing before the Senate Committee on Homeland Security and Governmental Affairs
“Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland”
September 10, 2014**

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

Thank you Chairman Carper, Ranking Member Coburn, and members of the Committee. I appreciate this opportunity to be here today to discuss the terrorist threat against the United States and our efforts to counter it.

I also want to express my appreciation to the Committee for its unflagging support of the men and women at the National Counterterrorism Center. I am particularly pleased to be here today with Undersecretary Taylor, Undersecretary Spaulding, and Executive Assistant Director Anderson who are representing two of our closest partner agencies—the Department of Homeland Security and the Federal Bureau of Investigation. Together we are a part of the broader counterterrorism community that is more integrated and more collaborative than ever.

Earlier this summer the 9/11 Commissioners released their most recent report, and asked national security leaders to “communicate to the public—in specific terms—what the threat is, and how it is evolving.” With this in mind, Director Olsen recently had an opportunity to provide a sobering but objective assessment of Islamic State of Iraq and the Levant’s (ISIL’s) maturation and capability at the Brookings Institution. I similarly think hearings like this are an opportunity to continue this constructive dialogue with the public and their elected representatives.

The Overall Terrorist Threat

In May, the President told the graduating class of West Point cadets, “For the foreseeable future, the most direct threat to America at home and abroad remains terrorism.” The 9/11 Commissioners agreed noting in their July report, “the terrorist threat is evolving, not defeated.” From my vantage point at the National Counterterrorism Center, I would agree. Since we testified before this committee last year, the terrorist threat has evolved, is more geographically diffuse, and involves a greater diversity of actors.

Overseas, the United States faces an enduring threat to our interests, as evidenced by precautionary measures taken at some of our overseas installations. The threat emanates from a broad geographic area, spanning South Asia, across the Middle East, and much of North Africa, where terrorist networks have exploited a lack of governance and lax security.

Here in the United States, last year’s attack against the Boston Marathon highlighted the danger posed by lone actors and insular groups not directly tied to terrorist organizations, as well as the difficulty of identifying these types of plots before they take place. The flow of more than 12,000 foreign fighters to Syria and Iraq with varying degrees of access to Europe and the United

States heightens our concern, as these individuals may eventually return to their home countries battle-hardened, radicalized, and willing to commit violence.

In the face of sustained counterterrorism pressure, core al-Qa'ida has adapted by becoming more decentralized and is shifting away from large-scale, mass casualty plots like the attacks of September 11, 2001. Al-Qa'ida has modified its tactics, encouraging its adherents to adopt simpler attacks that do not require the same degree of resources, training, and planning.

Instability in the Levant, Middle East, and across North Africa has accelerated this decentralization of the al-Qa'ida movement, which is increasingly influenced by local and regional factors and conditions. This diffusion has also led to the emergence of new power centers and an increase in threats by networks of like-minded violent extremists with allegiances to multiple groups. Ultimately, this less centralized network poses a more diverse and geographically dispersed threat and is likely to result in increased low-level attacks against U.S. and European interests overseas.

Today, I will begin by examining the terrorist threats to the homeland and then outline the threat to U.S. interests overseas. I will then focus the remainder of my remarks on outlining some of NCTC's efforts to address this complicated threat picture.

Threat to the Homeland

Starting with the homeland, we remain concerned about terrorist groups' efforts to target Western aviation. In early July, the United States and United Kingdom implemented enhanced security measures at airports with direct flights to the United States, which included new rules aimed at screening personal electronic devices. This past winter, additional security measures surrounding commercial aviation were implemented to address threats to the Sochi Olympics. Although unrelated, taken together these two instances are illustrative of the fact that terrorist groups continue to see commercial aviation as a desirable symbolic target, and these aspirations are not limited to Al-Qa'ida in the Arabian Peninsula.

Nevertheless, we do assess that AQAP remains the al-Qa'ida affiliate most likely to attempt transnational attacks against the United States. The group's repeated efforts to conceal explosive devices to destroy aircraft demonstrate its longstanding interest in targeting Western aviation. Its three attempted attacks demonstrate the group's continued pursuit of high-profile attacks against the West, its awareness of Western security procedures, and its efforts to adapt.

Despite AQAP's ambitions, Homegrown Violent Extremists (HVEs) remain the most likely immediate threat to the homeland. The overall level of HVE activity is likely to stay the same: a handful of uncoordinated and unsophisticated plots emanating from a pool of up to a few hundred individuals. Lone actors or insular groups who act autonomously pose the most serious HVE threat, and we assess HVEs will likely continue gravitating to simpler plots that do not require advanced skills, outside training, or communications with others.

The Boston Marathon bombing underscores the threat from HVEs who are motivated to act violently by themselves or in small groups. In the months prior to the attack, the Boston Marathon bombers exhibited few behaviors that law enforcement and intelligence officers

traditionally used to detect readiness to commit violence. The perceived success of previous lone offender attacks combined with al-Qa'ida's and AQAP's propaganda promoting individual acts of terrorism is raising the profile of this tactic.

HVEs make use of a diverse online environment that is dynamic, evolving, and self-sustaining. This online environment is likely to play a critical role in the foreseeable future in radicalizing and mobilizing HVEs towards violence. Despite the removal of important terrorist leaders during the last several years, the online environment continues to reinforce a violent extremist identity, supplies grievances, and provides HVEs the means to connect with terrorist groups overseas.

This boundless virtual environment, combined with terrorists' increasingly sophisticated use of social media, makes it increasingly difficult to protect our youth from sometimes horrifically brutal propaganda. ISIL's online media presence has become increasingly sophisticated, disseminating timely, high-quality media content across multiple platforms.

The Islamic State of Iraq and the Levant (ISIL)

ISIL is a terrorist organization that has exploited the conflict in Syria and sectarian tensions in Iraq to entrench itself in both countries. The group's strength and expansionary agenda pose an increasing threat to our regional allies and to U.S. facilities and personnel in both the Middle East and the West.

ISIL's goal is to solidify and expand its control of territory and govern by implementing its violent interpretation of *sharia* law. The group aspires to overthrow governments in the region, govern all the territory that the early Muslim caliphs controlled, and expand even further. ISIL's claim to have re-established the caliphate demonstrates the group's desire to lead violent extremists around the world.

Then Iraq-based ISIL exploited the conflict and chaos in Syria to expand its operations across the border. The group, with al-Qaida's approval, established the al-Nusrah Front as a cover for its Syria-based activities but in April 2013, publicly declared its presence in Syria under the ISIL name. ISIL accelerated its efforts to overthrow the Iraqi government, seizing control of Fallujah this past January. The group marched from its safe haven in Syria and across the border into northern Iraq, killing thousands of Iraqi Muslims on its way to seizing Mosul this June.

Along the way, ISIL aggressively recruited new adherents. Some joined ISIL to escape Assad's brutal treatment and oppression of his own people. Others joined out of frustration, marginalized by their own government. But many joined out of intimidation and fear, forced to choose either obedience to ISIL or a violent, oftentimes public death.

The withdrawal of Iraqi Security Forces during those initial military engagements has left ISIL with large swaths of ungoverned territory. It has established sanctuaries in Syria and Iraq from where they plan, train, and plot terrorist acts with little interference. Our latest assessment of ISIL's strength places the group at more than 10,000 members. Sunni groups that ISIL is

fighting with in Iraq also augment the group's strength in that battlefield. ISIL's control over the Iraq-Syria border enables the group to easily move members between Iraq and Syria, which can rapidly change the number of fighters in either country. ISIL is also drawing some recruits from the more than 12,000 foreign fighters who have traveled to Syria.

ISIL's recent victories have provided the group with a wide array of weapons, equipment, and other resources. Battlefield successes also have given ISIL an extensive war chest, which as of early this month probably includes around \$1 million per day in revenues from black-market oil sales, smuggling, robberies, and ransom payments for hostages.

Notably, ISIL has sought to call into question the legitimacy of Ayman al-Zawahiri's succession of Usama bin Laden. While al-Qa'ida core remains the ideological leader of the global terrorist movement, its primacy is being challenged by the rise of ISIL whose territorial gains, increasing access to a large pool of foreign fighters, and brutal tactics are garnering significantly greater media attention. We continue to monitor for signs of fracturing within al-Qa'ida's recognized affiliates.

ISIL's safe haven in Syria and Iraq and the group's access to resources pose an immediate and direct threat to U.S. personnel and facilities in the region. This includes our embassy in Baghdad and our consulate in Erbil—and, of course, it includes the Americans held hostage by ISIL.

But ISIL's threat extends beyond the region, to the West. This January, ISIL's leader publicly threatened "direct confrontation" with the U.S., and has repeatedly taunted Americans, most recently through the horrifically graphic execution of two journalists who were reporting on the plight of the Syrian people. In Europe, the arrest of an ISIL-connected individual in France who possessed several explosive devices and a shooting in Brussels by an ISIL-trained fighter clearly demonstrate this threat, and the threat returning foreign fighters pose.

The FBI has arrested more than half a dozen individuals seeking to travel from the U.S. to Syria to support ISIL. We remain mindful of the possibility that an ISIL-sympathizer could conduct a limited, self-directed attack here at home with no warning.

Al-Qa'ida Core and Afghanistan/Pakistan-based Groups

Turning now to core al-Qa'ida and Afghanistan/Pakistan-based groups, we anticipate that despite core al-Qa'ida's diminished leadership cadre, remaining members will continue to pose a threat to Western interests in South Asia and would attempt to strike the homeland should an opportunity arise. Al-Qa'ida leader Ayman al-Zawahiri's public efforts to promote individual acts of violence in the West have increased, as the Pakistan-based group's own capabilities have diminished.

Despite ISIL's challenge, Zawahiri remains the recognized leader of the global jihadist movement among al-Qa'ida affiliates and allies, and the groups continue to defer to his guidance on critical issues. Since the start of the Arab unrest in North Africa and the Middle East,

Zawahiri and other members of the group's leadership have directed their focus there, encouraging cadre and associates to support and take advantage of the unrest.

South Asia-Based Militants. Pakistani and Afghan militant groups—including Tehrik-e Taliban Pakistan (TTP), the Haqqani Network, and Lashkar-e Tayyiba (LT)—continue to pose a direct threat to U.S. interests and our allies in the region, where these groups probably will remain focused. We continue to watch for indicators that any of these groups, networks, or individuals are actively pursuing or have decided to incorporate operations outside of South Asia as a strategy to achieve their objectives.

TTP remains a significant threat in Pakistan despite the ongoing Pakistan military operations in North Waziristan and leadership changes during the past year. Its claim of responsibility for the June attack on the Jinnah International Airport in Karachi that killed about 30 people underscores the threat the group poses inside the country.

The Haqqani network is one of the most capable and lethal terrorist groups in Afghanistan and poses a serious threat to the stability of the Afghan state as we approach 2014 and beyond. Last month, the Department of State listed four high-ranking Haqqani members—Aziz Haqqani, Khalil Haqqani, Yahya Haqqani, and Qari Abdul Rauf—on the “Rewards for Justice” most-wanted list for their involvement in terrorist attacks in Afghanistan and ties to al-Qa’ida. The Haqqanis have conducted numerous high-profile attacks against U.S., NATO, Afghan Government, and other allied nation targets. In October 2013, Afghan security forces intercepted a truck bomb deployed by the Haqqanis against Forward Operating Base Goode in the Paktiya Province. The device, which did not detonate, contained some 61,500 pounds of explosives and constitutes the largest truck bomb ever recovered in Afghanistan.

Lashkar-e-Tayyiba (LT) remains focused on its regional goals in South Asia. The group is against improving relations between India and Pakistan, and its leaders consistently speak out against India and the United States, accusing both countries of trying to destabilize Pakistan. LT has attacked Western interests in South Asia in pursuit of its regional objectives, as demonstrated by the targeting of hotels frequented by Westerners during the Mumbai attacks in 2008. LT leaders almost certainly recognize that an attack on the U.S. would result in intense international backlash against Pakistan and endanger the group's safe haven there. However, LT also provides training to Pakistani and Western militants, some of whom could plot terrorist attacks in the West without direction from LT leadership.

Al-Qa’ida Affiliates

AQAP. Al-Qa’ida in the Arabian Peninsula (AQAP) remains the affiliate most likely to attempt transnational attacks against the United States. AQAP's three attempted attacks against the United States to date—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot in May 2012—demonstrate the group's continued pursuit of high-profile attacks against the United States. In a propaganda video released in March, the group's leader threatened the U.S. in a speech to recruits in Yemen, highlighting AQAP's persistent interest in targeting the United States.

AQAP also presents a high threat to U.S. personnel and facilities in Yemen and Saudi Arabia. In response to credible al-Qa'ida threat reporting in August 2013, the State Department issued a global travel alert and closed U.S. embassies in the Middle East and North Africa as part of an effort to take precautionary steps against such threats. We assess that we at least temporarily delayed this particular plot, but we continue to track closely the status of AQAP plotting against our facilities and personnel in Yemen. AQAP continues to kidnap Westerners in Yemen and carry out numerous small-scale attacks and large-scale operations against Yemeni government targets, demonstrating the range of the group's capabilities. In addition, this past July AQAP launched its first successful attack in Saudi Arabia since 2009, underscoring the group's continued focus on operations in the Kingdom.

Finally, AQAP continues its efforts to radicalize and mobilize to violence individuals outside Yemen through the publication of its English-language magazine *Inspire*. Following the Boston Marathon bombings, AQAP released a special edition of the magazine claiming that accused bombers Tamarlan and Dzhokhar Tsarnaev were "inspired by *Inspire*," highlighting the attack's simple, repeatable nature, and tying it to alleged U.S. oppression of Muslims worldwide. The most recent *Inspire* issue in March—AQAP's twelfth—continued to encourage "lone offender" attacks in the West, naming specific targets in the United States, United Kingdom, and France and providing instructions on how to construct a vehicle-borne improvised explosive device.

Al-Shabaab. We continue to monitor al-Shabaab and its foreign fighter cadre as a potential threat to the U.S. homeland, as some al-Shabaab leaders have publicly called for transnational attacks and the group has attracted dozens of U.S. persons—mostly ethnic Somalis—who have traveled to Somalia since 2006. The death of al-Shabaab's leader Ahmed Abdi in a recent strike by U.S. military forces raises the possibility of potential retaliatory attacks against our personnel and facilities in East Africa.

Al-Shabaab is mainly focused on undermining the Somali Federal Government and combating African Mission in Somalia (AMISOM) and regional military forces operating in Somalia. While al-Shabaab's mid-September 2013 attack on the Westgate mall in Kenya demonstrated that the group continues to plot against regional and Western targets across East Africa, as part of its campaign to remove foreign forces aiding the Somali Government.

AQIM and regional allies. Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) and its allies remain focused on local and regional attack plotting, including targeting Western interests. The groups have shown minimal interest in targeting the U.S. homeland.

In Mali, the French-led military intervention has pushed AQIM and its allies from the cities that they once controlled, but the groups maintain safe haven in the less populated areas of northern Mali from which they are able to plan and launch attacks against French and allied forces in the region. Elsewhere, AQIM is taking advantage of permissive operating environments across much of North Africa to broaden its reach. We are concerned that AQIM may be collaborating with local violent extremists, including Ansar al-Sharia groups in Libya and Tunisia.

In August of last year, two highly capable AQIM offshoots, Mokhtar Belmokhtar's al-Mulathamun battalion and Tawhid Wal Jihad in West Africa, merged to form the new violent extremist group—al-Murabitun—which will almost certainly seek to conduct additional high profile attacks against Western interests across the region. Belmokhtar—the group's external operations commander—played a leading role in attacks against Western interests in Northwest Africa in 2013, with his January attack on an oil facility in In-Amenas, Algeria and double suicide bombings in Niger in May. Early this year, Belmokhtar relocated from Mali to Libya to escape counterterrorism pressure, and probably to collaborate with Ansar al-Sharia (AAS) and other violent extremist elements in the country to advance his operational goals.

Boko Haram is waging unprecedented violence in northeast Nigeria this year and is expanding its reach into other parts of Nigeria and neighboring states to implement its harsh version of *sharia* law and suppress the Nigerian Government and regional CT pressure. Since late 2012, Boko Haram and its splinter faction Ansaru have claimed responsibility for five kidnappings of Westerners, raising their international profile and highlighting the threat they pose to Western and regional interests. Boko Haram has kidnapped scores of additional Nigerians in northeast Nigeria since the kidnapping of 276 school girls from Chibok, Nigeria in April 2014.

Al Nusrah Front. Al-Nusrah Front is one of the most capable groups within the Syrian opposition and has mounted suicide, explosive, and firearms attacks against regime and security targets across the country; it has also sought to provide limited public services and governance to the local population in areas under its control. Several Westerners have joined al-Nusrah Front, including a few who have perished in suicide operations, raising concerns capable individuals with extremist contacts and battlefield experience could return to their home countries to commit violence. In April 2013, Al-Nusrah Front's leader, Abu Muhammad al-Jawlani, pledged allegiance to al-Qa'ida leader Ayman al-Zawahiri, publicly affirming the group's ties to core al-Qa'ida. Al-Zawahiri named the group al-Qaida's recognized affiliate in the region later last year, ordering ISIL to return to Iraq.

Al-Qa'ida in the Indian Subcontinent. This month, al-Qa'ida announced the establishment of its newest affiliate, al-Qa'ida in the Indian Subcontinent (AQIS). Al-Qa'ida used social media and online web forums to make known the existence of AQIS, which al-Qa'ida said it has worked for more than two years to create. We assess the creation of AQIS is not a reaction to al-Qa'ida's split with ISIL, though the timing of the announcement may be used to bolster al-Qa'ida's standing in the global jihad movement. AQIS, which is led by Sheikh Asim Umer, has stated objectives that include violence against the U.S., establishing Islamic law in South Asia, ending occupation of Muslim lands, and defending Afghanistan under Mullah Omar's leadership.

Threat from Shia Groups

Iran and Hizballah remain committed to defending the Assad regime, including sending billions of dollars in military and economic aid, training pro-regime and Shia militants, and

deploying their own personnel into the country. Iran and Hizballah view the Assad regime as a key partner in an “axis of resistance” against Israel and the West and are prepared to take major risks to preserve the regime as well as their critical transshipment routes.

Lebanese Hizballah. In May of last year, Hizballah publicly admitted that it is fighting for the Syrian regime and its chief, Hasan Nasrallah, framed the war as an act of self-defense against Western-backed Sunni violent extremists. Hizballah continues sending capable fighters for pro-regime operations and support for a pro-regime militia. Additionally, Iran and Hizballah are leveraging allied Iraqi Shi’a militant and terrorist groups to participate in counter-opposition operations. This active support to the Assad regime is driving increased Sunni violent extremist attacks and sectarian unrest in Lebanon.

Beyond its role in Syria, Lebanese Hizballah remains committed to conducting terrorist activities worldwide and we remain concerned the group’s activities could either endanger or target U.S. and other Western interests. The group has engaged in an aggressive terrorist campaign in recent years and continues attack planning abroad. In April 2014, two Hizballah operatives were arrested in Thailand and one admitted that they were there to carry out a bomb attack against Israeli tourists, underscoring the threat to civilian centers.

Iranian Threat. In addition to its role in Syria, Iran remains the foremost state sponsor of terrorism, and works through the Islamic Revolutionary Guard Corps-Qods Force and Ministry of Intelligence and Security to support groups that target U.S. and Israeli interests globally. In March, Israel interdicted a maritime vessel that departed Iran and was carrying munitions judged to be intended for Gaza-based Palestinian militants. Iran, largely through Qods Force Commander Soleimani, has also provided support to Shia militias and the Iraqi government to combat ISIL in Iraq.

Iran continues to be willing to conduct terrorist operations against its adversaries. This is demonstrated by Iran’s links to terrorist operations in Azerbaijan, Georgia, India, and Thailand in 2012. Iran also continues to provide lethal aid and support the planning and execution of terrorist acts by other groups, in particular Lebanese Hizballah.

Taken together, the current threat landscape is a manifestation of the transformation of the global jihadist movement over the past several years. This movement has diversified and expanded in the aftermath of the upheaval and political chaos in the Arab world since late 2010. The threat now comes from a more decentralized array of organizations and networks.

NCTC’s Counterterrorism Efforts

The United States, United Kingdom, France, and the broader international community have increasingly expressed concerns about the greater than 12,000 foreign fighters who could potentially return to their home countries to participate in or support terrorist attacks. The UK’s Home Secretary announced the terrorist threat level in the United Kingdom had been raised to severe, explaining, “The increase in threat level is related to developments in Syria and Iraq where terrorist groups are planning attacks against the West. Some of those plots are likely to

involve foreign fighters who have traveled there from the UK and Europe to take part in those conflicts.”

Syria remains the preeminent location for independent or al-Qa’ida-aligned groups to recruit, train, and equip a growing number of extremists, some of whom we assess may seek to conduct external attacks. The rate of travelers into Syria exceeds the rate of travelers who went into Afghanistan/Pakistan, Iraq, Yemen, or Somalia at any point in the last ten years.

European governments estimate that more than 2,000 westerners have traveled to join the fight against the Assad regime, which includes more than 500 from Great Britain, 700 from France, and 400 from Germany. Additionally, over 100 U.S. persons from a variety of backgrounds and locations in the United States have traveled or attempted to travel to Syria.

NCTC, FBI, and DHS are part of a broader U.S. government and international effort to resolve the identities of potential violent extremists and identify potential threats emanating from Syria. As you know, this committee and the Congress charged NCTC with maintaining the U.S. government’s central and shared knowledge bank of known and suspected international terrorists (or KSTs), their contacts, and their support networks. To manage this workload, NCTC developed a database called TIDE – the Terrorist Identities Datamart Environment.

TIDE is much more than a screening database – it is an analytic database. It feeds the unclassified screening database so that DHS, the State Department, and other agencies have timely and accurate information about known and suspected terrorists. As disparate pieces of information about KSTs are received, trained analysts create new records, most often as the result of a nomination by a partner agency. The records are updated—or “enhanced”—regularly as new, related information is included and dated or as unnecessary information is removed. In all cases, there are several layers of review before a nomination is accepted into the system. In the case of U.S. persons, there are at least four layers of review, including a legal review, to ensure the derogatory information is sufficient and meets appropriate standards.

To better manage and update the identities of individuals who have travelled overseas to engage in violence in Syria and Iraq, we’ve created a special threat case in TIDE. This is a special feature in the TIDE system which allows us to focus efforts on smaller groups of individuals. A threat case links all known actors, and their personal information, involved in a particular threat stream or case and makes that information available to the intelligence, screening, and law enforcement communities.

NCTC’s management of this unique consolidation of terrorist identities has created a valuable forum for identifying and sharing information about Syrian foreign fighters—including ISIL—with community partners. It has better integrated the community’s efforts to identify, enhance, and expedite the nomination of Syrian foreign fighter records to the Terrorist Screening Database for placement in U.S. government screening systems.

Counterterrorism efforts focused on law enforcement disruptions are critical to mitigating threats. We also recognize that government alone cannot solve this problem and interdicting or arresting terrorists is not the full solution. Well-informed and well-equipped families,

communities, and local institutions represent the best long-term defense against violent extremism.

To this end, we continue to refine and expand the preventive side of counterterrorism. Working with DHS, in the last year NCTC revamped the Community Awareness Briefing (CAB), a key tool we use to convey information to local communities and authorities on the terrorist recruitment threat. The CAB now also includes information on the recruitment efforts of violent extremist groups based in Syria and Iraq. Additionally, this year NCTC and DHS developed and implemented a new program – the Community Resilience Exercise program, designed to improve communication between law enforcement and communities and to share ideas on how to counter violent extremism.

Conclusion

Confronting these threats and working with resolve to prevent another terrorist attack remains the counterterrorism community's overriding mission. This year, NCTC celebrates its 10th year in service to the nation, and while the Center has matured tremendously over that period, we are focused on positioning ourselves to be better prepared to address the terrorist threat in decades to come.

Chairman Carper, Ranking Member Coburn, 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.

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



Department of Justice

STATEMENT OF

**ROBERT ANDERSON, JR.
EXECUTIVE ASSISTANT DIRECTOR
CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE**

BEFORE THE

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

ENTITLED

**"CYBERSECURITY, TERRORISM, AND BEYOND:
ADDRESSING EVOLVING THREATS TO THE HOMELAND"**

PRESENTED

SEPTEMBER 10, 2014

**Statement of
Robert Anderson, Jr.
Executive Assistant Director
Criminal, Cyber, Response, and Services Branch
Federal Bureau of Investigation
Department of Justice**

**Before the
Committee on Homeland Security and Governmental Affairs
United States Senate**

**Entitled
“Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland”**

**Presented on
September 10, 2014**

Good morning Chairman Carper and Ranking Member Coburn. I appreciate the opportunity to appear before you today to discuss cyber, terrorism, and other threats to our nation and how the FBI is collaborating with our partners in government, law enforcement, and the private sector to prevent and combat them.

The Cyber Threat and FBI Response

We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our economy.

Given the scope of the cyber threat, agencies across the Federal government are making cyber security a top priority. We and our partners at the Department of Homeland Security (DHS), the National Security Agency, and other U.S. Intelligence Community and law enforcement agencies have truly undertaken a whole-of-government effort to combat the cyber threat. Within the FBI, we are prioritizing high-level intrusions—the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We are working with our counterparts to predict and prevent attacks, rather than simply react after the fact.

FBI agents, analysts, and computer scientists use technical capabilities and traditional investigative techniques—such as sources and wiretaps, surveillance, and forensics—to fight cyber crime. We work side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and at the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24-hour cyber command center, CyWatch, 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 significant cyber intrusion.

We also exchange information about cyber threats with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance (NCFTA).

For our partners in State and local law enforcement, we have launched Cyber Shield Alliance on www.leo.gov, which provides access to cyber training opportunities and information, as well as the ability to report cyber incidents to the FBI.

In addition, our legal attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting and collaborating with newly established cyber crime centers at Interpol and Europol. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe.

We know that to be successful in the fight against cyber crime, we must continue to recruit, develop, and retain a highly skilled workforce. To that end, we have developed a number of innovative staffing programs and collaborative private industry partnerships to ensure that over the long term we remain focused on our most vital resource—our people.

As the committee is well aware, the frequency and impact of cyber attacks on our nation's private sector and government networks have increased dramatically in the past decade, and are expected to continue to grow. Since 2002, the FBI has seen an 80 percent increase in the number of computer intrusion investigations.

Recent Successes

Over the past several months, the FBI and the Justice Department have announced a series of separate indictments of overseas cyber criminals.

In an unprecedented indictment in May, we charged five Chinese hackers with illegally penetrating the networks of six U.S. companies. The five members of China's People's Liberation Army allegedly used their illegal access to exfiltrate proprietary information, including trade secrets.

Later that month, we announced the indictments of a Swedish national and a U.S. citizen believed to be the co-developers of a particularly insidious computer malware known as Blackshades. This software was sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide.

In June, the FBI announced a multinational effort to disrupt the GameOver Zeus botnet, the most sophisticated botnet that the FBI and its allies had ever attempted to disrupt. GameOver Zeus is believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world. This effort to disrupt it involved notable cooperation with the

private sector and international law enforcement. GameOver Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to GameOver Zeus are estimated to be more than \$100 million.

Just last month, a Federal grand jury indicted Su Bin, a Chinese national, on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft. Su is currently in custody in British Columbia, Canada, where he is being held pursuant to a provisional arrest warrant submitted by the United States. The charges carry a total maximum statutory penalty of 30 years in prison. The investigation in this case was conducted by the Federal Bureau of Investigation and the Air Force Office of Special Investigations.

The Blackshades and GameOver Zeus indictments are part of an initiative launched by the FBI Cyber Division in April 2013 to disrupt and dismantle the most significant botnets threatening the economy and national security of the United States. This initiative, named Operation Clean Slate, is the FBI's broad campaign to implement appropriate threat neutralization actions through collaboration with the private sector, DHS, and other United States government partners, as well as our foreign partners. This includes law enforcement action against those responsible for the creation and use of the illegal botnets, mitigation of the botnet itself, assistance to victims, public service announcements, and long-term efforts to improve awareness of the botnet threat through community outreach. Although each botnet is unique, Operation Clean Slate's strategic approach to this significant threat ensures a comprehensive neutralization strategy, incorporating a unified public/private response and a whole-of-government approach to protect U.S. interests.

The impact of botnets has been significant. Botnets have been estimated to cause more than \$113 billion in losses globally, with approximately 375 million computers infected each year, equaling more than one million victims per day, translating to 12 victims per second.

Another Operation Clean Slate success came in January 2014, when Aleksandry Andreevich Panin, a Russian national, pled guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the malicious software known as Spyeye, which infected more than 1.4 million computers in the United States and abroad. Based on information received from the financial services industry, more than 10,000 bank accounts had been compromised by Spyeye infections in 2013 alone. Panin's co-conspirator, Hamza Bendelladj, an Algerian national who helped Panin develop and distribute the malware, was also arrested in January 2013 in Bangkok, Thailand.

In addition to these recent investigative successes against cyber threats, we are continuing to work with our partners to prevent attacks before they occur.

One area in which we have had great success with our overseas partners is in identifying and targeting infrastructure we believe has been used in distributed denial of service (DDoS) attacks,

and preventing that infrastructure from being used for future attacks. A DDoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network.

Since October 2012, the FBI and DHS have released more than 170,000 Internet Protocol addresses of computers that were believed to be infected with DDoS malware. We have released this information through Joint Indicator Bulletins (JIBs) to more than 130 countries via DHS's National Cybersecurity and Communications Integration Center (NCCIC), where our liaisons provide expert and technical advice for increased coordination and collaboration, as well as to our legal attachés overseas.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDoS attacks. We are continuing to target botnets through this strategy and others.

In 2013, for example, the FBI created FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs) to release industry-specific details on current and emerging threat trends, and technical indicators to the private sector. To date, the FBI has disseminated 40 FLASH messages, 21 of which dealt with threats to the financial industry. These PIN and FLASH messages were created to proactively deliver timely, actionable intelligence to potential victims and law enforcement partners at the international, State, and local levels.

Next Generation Cyber Initiative

The need to prevent attacks is a key reason the FBI has redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next Generation Cyber Initiative, which we launched in 2012, entails a wide range of measures, including focusing the Cyber Division on intrusions into computers and networks—as opposed to crimes committed with a computer as a modality hiring additional computer scientists to assist with technical investigations in the field; and expanding partnerships and collaboration at the NCIJTF. In addition, after more than a decade of combating cybercrime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces in all 56 field offices to focus exclusively on cybersecurity threats.

At the 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—we are coordinating at an unprecedented level. This coordination involves senior personnel at key agencies. NCIJTF, which is led by the FBI, now has deputy directors from the NSA, DHS, the Central Intelligence Agency, U.S. Secret Service, and U.S. Cyber Command. In the past year, three of our Five Eyes international partners joined us at the NCIJTF: Australia embedded a liaison officer in May 2013, the UK in July 2013, and Canada in January 2014. By developing partnerships with these and other nations, NCIJTF is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries.

Private Sector Outreach

In addition to strengthening our partnerships in government and law enforcement, we recognize that to effectively combat the cyber threat, we must significantly enhance our collaboration with the private sector. Our nation's companies are the primary victims of cyber intrusions, and their networks contain the evidence of countless attacks. In the past, industry has provided us information about attacks that have occurred, and we have investigated the attacks—but we have not always provided information back.

To remedy that, the Cyber Division has established a Key Partnership Engagement Unit (KPEU) to manage a targeted outreach program focused on building relationships with key private sector corporations. The unit works to share sector-specific threat information with our corporate partners.

We have provided a series of classified briefings for key sectors, including financial services and energy, to help them repel intruders.

Through the FBI's InfraGard program, the FBI develops partnerships and working relationships with private sector, academic, and other public-private entity subject matter experts. Primarily geared toward the protection of critical national infrastructure, InfraGard promotes ongoing dialogue and timely communication among a current active membership base of more than 25,000.

InfraGard members are encouraged to share information with government that better allows government to prevent and address criminal and national security issues. Active members are able to report cyber intrusion incidents in real-time to the FBI through iGuardian, which is based on our successful counterterrorism reporting system known as Guardian.

Just last month, the FBI deployed a malware repository and analysis system called Malware Investigator to our domestic and foreign law enforcement partners and members of the U.S. Intelligence Community. The system allows users to submit malware directly to the FBI and quickly receive technical information about the samples to its users so they can understand how the malware works. It also enables the FBI to obtain a global view of the malware threat. Beyond technical reporting, Malware Investigator identifies correlations that will allow users to "connect the dots" by highlighting instances in which malware was deployed in seemingly unrelated incidents.

The FBI's Cyber Initiative and Resource Fusion Unit (CIRFU) maximizes and develops intelligence and analytical resources received from law enforcement, academia, international, and critical corporate private sector subject matter experts to identify and combat significant actors involved in current and emerging cyber-related criminal and national security threats. CIRFU's core capabilities include a partnership with the National Cyber Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania, where the unit is collocated with CIRFU. NCFTA acts as a neutral platform through which the unit develops and maintains liaison with hundreds of formal and informal working partners who share real-time threat information and

best practices and collaborate on initiatives to target and mitigate cyber threats domestically and abroad.

The FBI recognizes that industry collaboration and coordination are critical in our combating the cyber threat effectively. As part of our enhanced private sector outreach, we have begun to provide cleared industry partners with classified threat briefings and other information and tools to better help them repel intruders.

Counterterrorism and Other Threats

Though the cyber threat is one of the FBI's top priorities, combating terrorism remains our top investigative priority. As geopolitical conflict zones continue to emerge throughout many parts of the world, terrorist groups may use this instability to recruit and incite acts of violence.

The continuing violence in both Syria and Iraq and the influx of foreign fighters threatens to destabilize an already volatile region while also heightening the threat to the West. Due to the prolonged nature and the high visibility of the Syrian conflict, we are concerned that U.S. persons with an interest in committing jihad will be drawn to the region. We can address this issue more fully in the closed session.

In conclusion, Chairman Carper, to counter the threats we face, we are engaging in an unprecedented level of collaboration within the U.S. government, with the private sector, and with international law enforcement.

We are grateful for the committee's support and look forward to continuing to work with you and expand our partnerships to defeat our adversaries.

9/12/2014

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program : NPR *submitted by Sen. Baldwin*

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program

by AREZOU REZVANI, JESSICA PUPOVAC, DAVID EADS and TYLER FISHER

September 02, 2014 6:09 PM ET

Amid widespread criticism of the deployment of military-grade weapons and vehicles by police officers in Ferguson, Mo., President Obama recently ordered a review of federal efforts supplying equipment to local law enforcement agencies across the country.

So, we decided to take a look at what the president might find.

NPR obtained data from the Pentagon on every military item sent to local, state and federal agencies through the Pentagon's Law Enforcement Support Office — known as the 1033 program — from 2006 through April 23, 2014. The Department of Defense does not publicly report which agencies receive each piece of equipment, but they have identified the counties that the items were shipped to, a description of each, and the amount the Pentagon initially paid for them.

We took the raw data, analyzed it and have organized it to make it more accessible. We are making that data set available to the public today.

Here's what we found:

1. Gear: MRAPs, Bayonets And Grenade Launchers

The 1033 program is the key source of the most visible, big-ticket, military item being sent to local law enforcement: mine-resistant, ambush-protected vehicles, or MRAPs. Designed to withstand bullets, grenades and roadside bombs on the front lines of war, more than 600 of them have been sent to local law enforcement agencies in almost every state in the U.S., mostly within the past year. Los Angeles County, for example, has nine of these vehicles, six of which were obtained just this past March.

But the program is a conduit for much more than just MRAPs. Since 2006, through the 1033 program, the Pentagon has also distributed:

79,288 assault rifles

<http://www.npr.org/2014/09/02/342494225/mrap-and-bayonets-what-we-know-about-the-pentagons-1033-program>

1/6

9/12/2014

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program : NPR

205 grenade launchers

11,959 bayonets

3,972 combat knives

\$124 million worth of night-vision equipment, including night-vision sniper scopes

479 bomb detonator robots

50 airplanes, including 27 cargo transport airplanes

422 helicopters

More than \$3.6 million worth of camouflage gear and other "deception equipment"

2. More Than Just Combat Gear

It turns out that weapons are a relatively small part of the 1033 program.

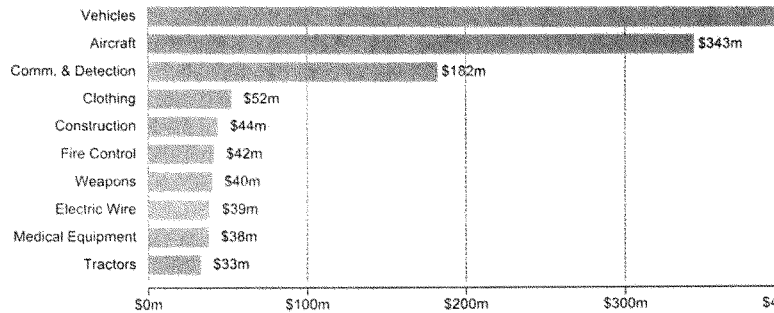
Each item in the database has a National Stock Number (NSN), which NPR used to determine the general category of each item and gain a broader understanding of what types of equipment have been made available through the 1033 program. The list includes building materials, musical instruments and even toiletries. (We've added those categories to the data we're publishing today.)

9/12/2014

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program : NPR

Top 10 categories by total cost to the Department of Defense

The Department of Defense categorizes every item in the 1033 program by its NSN, or National Stock Number. That National Stock Number contains the item's Federal Supply Category. Calculating the cost of every item in the program by its Federal Supply Category shows that vehicles have been the most expensive category for the Department of Defense by far.



Source: Defense Logistics Agency

Actual weaponry, not including vehicles of any kind, account for just over 3 percent of the total value of all goods sent out by the Pentagon between 2006 and April.

3. What The Data Don't Tell Us: Why?

Congress authorized the 1033 program in 1989 to equip local, state and federal agencies in the war on drugs. In 1996, Congress widened the program's scope to include counterterrorism. But the data do not confirm whether either of those public safety goals are, in fact, driving decisions about the distribution of equipment. Areas with large populations or high crime rates aren't necessarily receiving more or less than their share of the items. Nor is a greater amount of equipment being sent to areas along the U.S. borders or coasts, places more likely to be drug trafficking corridors or terrorist targets.

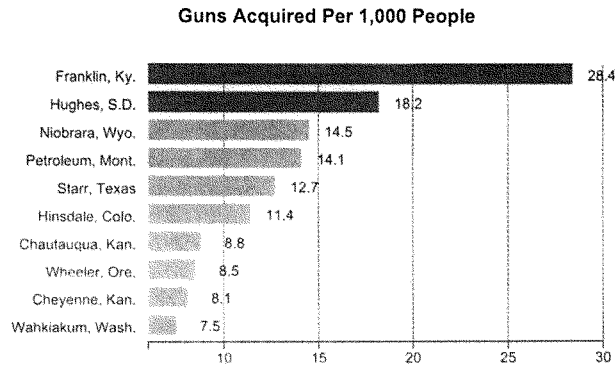
9/12/2014

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program : NPR

Top 10 U.S. Counties, guns acquired through 1033 program

Breaking down the number of guns acquired through the Pentagon's 1033 program by total count and guns per 1,000 people shows the prevalence of state capitals in the program. These weapons may have gone to state police and other state-level agencies.

State capital in county



Source: Gun numbers from the Defense Logistics Agency. Population statistics from the Census Bureau American Community Survey 5-year estimates.
Credit: David Eads and Tyler Fisher / NPR

Looking exclusively at who is getting what, the data don't clearly point to why certain agencies are receiving more surplus items than others.

Here's how it works: Equipment is posted to LESO's (the 1033 program office) website, and then local agencies can request it. Only state coordinators to the Defense Logistics Agency are tasked with approving or denying those requests.

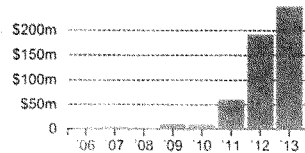
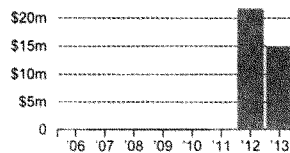
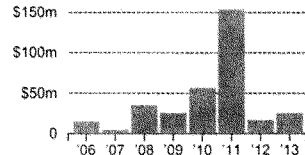
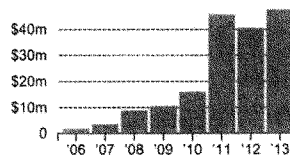
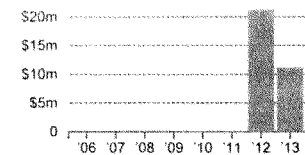
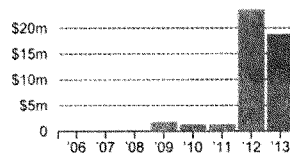
We did see trends in the data over time that show patterns of military overstocking and surplus.

9/12/2014

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program : NPR

Dollar Amount Of Items Distributed By Category, 2006-2013

These charts detail the distribution of equipment in the 10 most expensive categories over time.

Vehicles**Construction Equipment****Aircraft****Communications & Detection****Medical Equipment****Clothing****Electric Wire****Tractors****What The Data Don't Tell Us: The Local Story**

Our analysis of the data only took us so far. Many questions remain.

The data are merely a starting point for further exploration into why certain overstocked and surplus items are — and aren't — being requested. Questions remain about how and why they are being used, and the benefit, if any, to local law enforcement.

9/12/2014

MRAPs And Bayonets: What We Know About The Pentagon's 1033 Program : NPR

We've provided NPR member stations with the tools to begin asking these and other questions. With reporting at the national and local levels, we will continue to follow this story.

Editor's note at 2:30 p.m. ET, Sept. 3: A chart that explored the demographics of counties that have received equipment has been removed from this page. It wasn't intended to be part of this package and was inadvertently published before being finished. The data may be part of a future report.

Correction

Sept. 3, 2014

A previous version of the Total Guns Acquired chart stated that in Franklin County, Ky., guns acquired per 1,000 people were 28.3. It's actually 28.4 per 1,000 people.

pentagon

© 2014 NPR

Excerpted from information provided to NPR by LESO

WI	TREMPEALEAU	55121 2320-01-398-719 KIT, COMBAT IDE	2 Kit	1231
WI	TREMPEALEAU	55121 5895-01-518-886 KIT DUAL COM L	5 Kit	1174.2
WI	JUNEAU	55057 6350-01-477-768 KIT, INFRARED F	1 Each	12181
WI	ASHLAND	55003 1095-00-392-410 KNIFE, COMBAT,	3 EA	34.42
WI	BROWN	55009 6240-01-532-418 LAMP, INCANDES	10 Each	34.42
WI	MILWAUKEE	55079 6240-01-532-418 LAMP, INCANDES	4 Each	339.41
WI	MILWAUKEE	55079 6240-01-532-418 LAMP, INCANDES	3 Each	339.41
WI	MILWAUKEE	55079 6240-01-532-418 LAMP, INCANDES	4 Each	339.41
WI	MILWAUKEE	55079 6240-01-532-418 LAMP, INCANDES	30 Each	339.41
WI	MILWAUKEE	55079 6240-01-532-418 LAMP, INCANDES	2 Each	339.41
WI	MILWAUKEE	55079 6240-01-532-418 LAMP, INCANDES	20 Each	339.41
WI	DOOR	55029 7025-01-470-331 LAPTOP	2 Each	1940
WI	DOOR	55029 7021-00-RUG-GE LAPTOP RUGGI	50 EA	3139
WI	BROWN	55009 7045-DS-LAP-CA LAPTOP CASE	2 EA	50
WI	DOOR	55029 7021-DS-LAP-TC LAPTOP COMPL	12 Each	0
WI	CHIPPEWA	55017 1010-00-691-138 LAUNCHER, GRE	1 Each	720
WI	DANE	55025 1010-00-691-138 LAUNCHER, GRE	1 Each	720
WI	JACKSON	55053 1010-00-691-138 LAUNCHER, GRE	1 Each	720
WI	RACINE	55101 1010-00-691-138 LAUNCHER, GRE	1 Each	720
WI	RACINE	55101 1010-00-691-138 LAUNCHER, GRE	1 Each	720
WI	WAUKESHA	55133 1010-00-691-138 LAUNCHER, GRE	1 Each	720
WI	OCONTO	55083 3750-01-260-751 LAWN TRACTOF	1 EA	10940.35
WI	DOOR	55029 4220-01-474-515 LIFE PRESERVE	9 Each	517.48
WI	BROWN	55009 4220-01-379-615 LIFE PRESERVE	6 EA	42.28
WI	DANE	55025 4220-01-379-615 LIFE PRESERVE	4 EA	42.28
WI	EAU CLAIRE	55035 4220-01-379-615 LIFE PRESERVE	16 EA	42.28
WI	EAU CLAIRE	55035 4220-01-379-615 LIFE PRESERVE	2 EA	42.28
WI	IOWA	55049 4220-01-379-615 LIFE PRESERVE	12 EA	42.28
WI	WALWORTH	55127 4220-01-379-615 LIFE PRESERVE	4 EA	42.28
WI	DANE	55025 4220-01-056-866 LIFE RAFT, INFLJ	1 Each	608.48
WI	DANE	55025 4220-01-056-866 LIFE RAFT, INFLJ	1 Each	608.48
WI	DANE	55025 4220-01-056-866 LIFE RAFT, INFLJ	3 Each	608.48
WI	DOOR	55029 3930-DS-WHS-E LIFTALOFT AM	1 EA	8000
WI	OCONTO	55083 4940-DS-MSC-RI LIFT PLATFORM	1 EA	3689
WI	DOOR	55029 3930-DS-WHS-E LIFTALOFT SPW	1 EA	8000
WI	JACKSON	55053 5855-01-333-960 LIGHT AIMING K	2 Each	545.69
WI	JACKSON	55053 5855-01-333-960 LIGHT AIMING K	2 Each	545.69
WI	RACINE	55101 5855-01-333-960 LIGHT AIMING K	1 Each	545.69
WI	DOOR	55029 6220-01-527-724 LIGHT BAR	1 Each	832.7
WI	BROWN	55009 6230-01-589-482 LIGHT KIT, WEAF	2 Kit	7204.38

2462	#####	23 MOTOR VEHICLE	2320 Trucks and Truck Tractors, Wheeled
5871	216/2011 0:00:00	58 COMM/DETECT/	5895 Miscellaneous Communication Equipment
12181	#####	63 ALARM, SIGNAL	6350 Miscellaneous Alarm, Signal, and Security Detection S
103.26	#####	10 WEAPONS	1095 Miscellaneous Weapons
344.2	#####	10 WEAPONS	1095 Miscellaneous Weapons
1357.64	#####	62 LIGHTING FIXTL	6240 Electric Lamps
1018.23	#####	62 LIGHTING FIXTL	6240 Electric Lamps
1357.64	#####	62 LIGHTING FIXTL	6240 Electric Lamps
10182.3	#####	62 LIGHTING FIXTL	6240 Electric Lamps
678.82	#####	62 LIGHTING FIXTL	6240 Electric Lamps
6788.2	#####	62 LIGHTING FIXTL	6240 Electric Lamps
3880	#####	70 ADP EQPT/SOFT	7025 ADP Input/Output and Storage Devices
156950	#####	70 ADP EQPT/SOFT	7021 ADP Central Processing Unit (CPU, Computer), Digita
100	5/7/2012 0:00:00	70 ADP EQPT/SOFT	7045 ADP Supplies
0	3/5/2014 0:00:00	70 ADP EQPT/SOFT	1010 Guns, over 30 mm up to 75 mm
720	#####	10 WEAPONS	1010 Guns, over 30 mm up to 75 mm
720	#####	10 WEAPONS	1010 Guns, over 30 mm up to 75 mm
720	#####	10 WEAPONS	1010 Guns, over 30 mm up to 75 mm
720	6/9/2006 0:00:00	10 WEAPONS	1010 Guns, over 30 mm up to 75 mm
720	6/9/2006 0:00:00	10 WEAPONS	1010 Guns, over 30 mm up to 75 mm
720	#####	10 WEAPONS	1010 Guns, over 30 mm up to 75 mm
10940.35	4/5/2012 0:00:00	37 AGRICULTURAL	3750 Gardening Implements and Tools
4657.32	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
253.68	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
169.12	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
676.48	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
84.56	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
507.36	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
169.12	7/5/2012 0:00:00	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
608.48	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
608.48	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
1825.44	#####	42 FIRE/RESCUE/S,	4220 Marine Lifesaving and Diving Equipment
8000	#####	39 MATERIALS HAN	4220 Marine Lifesaving and Diving Equipment
3689	4/5/2012 0:00:00	49 MAINT/REPAIR S	3930 Warehouse Truck and Tractors, Self-Propelled
8000	#####	39 MATERIALS HAN	4940 Miscellaneous Maintenance and Repair Shop Speciali
1091.38	#####	58 COMM/DETECT/	3930 Warehouse Truck and Tractors, Self-Propelled
1091.38	#####	58 COMM/DETECT/	5855 Night Vision Equipment, Emitted and Reflected Radial
545.69	4/5/2007 0:00:00	58 COMM/DETECT/	5855 Night Vision Equipment, Emitted and Reflected Radial
832.7	#####	62 LIGHTING FIXTL	6220 Electric Vehicular Lights and Fixtures
14408.76	#####	62 LIGHTING FIXTL	6230 Electric Portable and Hand Lighting Equipment

Post-Hearing Questions for the Record
Submitted to Hon. Suzanne E. Spaulding & Hon. Francis X. Taylor
From Senator Claire McCaskill

**“Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the
Homeland”**
September 10, 2014

Question#:	1
Topic:	cyberattacks and hacking
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: During the hearing, Mr. Anderson noted the inevitability of cyberattacks and hacking against every federal agency.

Do the same policies, procedures and cybersecurity standards requirements to detect and deter attacks against federal agencies also apply to federal contractors, particularly contractors that handle national security sensitive and personally identifiable information? If not, why not, and what are the differences?

Response: The policies, procedures and standards applicable to federal agencies do not automatically apply to contractors. The Federal Information Security Management Act covers contractor systems holding Federal agency information, and clauses in individual contracts may require contractors to implement cybersecurity measures. For instance, if the contractors handle national security information, there are Department of Defense or Intelligence Community requirements that may apply. It is generally each agency’s responsibility to ensure that its contracts reflect the agency’s information security responsibilities.

Question#:	2
Topic:	ratio of contractors
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The threat to the homeland is ongoing, yet the rationale for contractors is usually to give agencies more flexibility over hiring and firing as the need for employees ebbs and flows.

How many contractors are involved in counterterrorism intelligence activities at DHS and what is the ratio of contractors to federal workers?

Response: Contractors are an essential part of the intelligence workforce, bringing specialized skills and providing needed workforce flexibility to respond to emerging threats. That said, it is important to maintain an appropriate balance between contractors and federal employees. The Office of Intelligence and Analysis (I&A) has transformed its workforce in recent years, significantly reducing its reliance on contractors. As recently as 2009, contractors represented over 60% of the intelligence workforce. As of the third quarter of Fiscal Year 2014, contractors comprise roughly 23% of the intelligence workforce. I&A will continue to evaluate its workforce to ensure an appropriate balance between contractors and federal employees.

Question#:	3
Topic:	contractors
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The threat to the homeland is ongoing, yet the rationale for contractors is usually to give agencies more flexibility over hiring and firing as the need for employees ebbs and flows.

Has any cost-benefit analysis been done to determine whether it's better to hire contractors or federal employees for particular positions? If so, please provide a copy of those analyses conducted and the results of those analyses.

Do you think that providing intelligence community contractors – who are doing the same or similar work as federal employees – with the same whistleblower protections that are available to federal employees would reduce the possibility of another Snowden-like leak to the press since contractors would be protected against retaliation if they used proper channels?

Response: Mission delivery and risk are primary factors in determining whether to hire a Federal employee or obtain contract services. The Department's Balanced Workforce Strategy (BWS) program comprises a set of processes that, when repeated on a regular basis, enables the Department to achieve the appropriate mix of federal employees and contractors to accomplish the Department's mission while minimizing mission risk that may result from an overreliance on contractors. The DHS BWS supports workforce planning and focuses on functions rather than particular positions. At DHS, a BWS analysis is required for all proposed service requirements greater than or equal to \$150,000, whether or not the requirements will lead to a services contract or a hiring action for a federal employee. Based on the BWS, when a Component determines that either federal employees or contractors would be suitable to perform a function, Components are responsible for considering and comparing the costs of government and contractor performance. This analysis provides "like comparisons" of costs and may influence the final decision on the most cost effective and efficient source of support for the Component. DHS continues to gain experience in using its tools and processes to support the appropriate mix of federal employees and contractors to accomplish the Department's mission.

It is unclear whether providing intelligence community contractors protections similar to federal employees would preclude a Snowden-like leak to the press. Data obtained through the Pilot Program may provide insight into that question.

Question#:	4
Topic:	DHS's Southern Border Plan
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing you mentioned the enhancement and integration of sensors as part of DHS's Southern Border Plan.

What specific lessons have been learned from GAO and internal DHS reports that are informing your Plan so that we do not continue to waste money on useless or overly expensive acquisitions when cheaper, more effective options may be available?

Please provide the Analysis of Alternatives for any planned acquisition involving ground sensors.

Response: The conclusions and lessons learned from GAO and internal DHS reports have focused on a few key themes. The first theme focuses on the utility of any system—we must take better steps to ensure that we are procuring systems that are cost-effective and that reflect the needs of the people who will use those systems to perform the mission. Another theme centers around discipline and rigor of the acquisition management process—we need to ensure our plans are well documented, scheduled, and priced—and then we need to ensure we have management systems in place to track our progress against those plans. Our management systems must also be capable of anticipating and heading off risks and issues, and of reacting effectively when we get off track from our plan. While we still have room for continued improvement, we believe we have made strong progress in responding to these themes and lessons learned.

In addition, we have our own lessons learned based on our own experiences and training. With respect to technology for the border, we recognized that we should not aspire to develop new systems, which will typically be costly, unless we are sure that we need new systems. We recognized that it is important to have flexibility so we can make trade-offs between the capabilities of a system and the cost. We needed a system that is the best value product or service that will meet our requirements. We concluded that a modular and tailored approach to technology deployments for each area of the border was more effective and less costly than an attempt to build a “one-size-fits-all” system that would cover the entire border.

As a result, we have re-designed our technology acquisitions for the border, focusing on a menu of available, non-developmental systems. Our acquisition strategies have created flexibilities so we can consider a wide variety of options at various levels of cost and capability. The results, to date, have resulted in significant cost reductions compared to our original estimates for these programs.

Question#:	4
Topic:	DHS's Southern Boarder Plan
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

We did conduct an Analysis of Alternatives for technology along the Southwest border.
We will work with your staff to make the documentation available for your review.

Question#:	5
Topic:	homegrown violent extremism
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: You state in your testimony that DHS is “[m]indful of the potential for homegrown violent extremism inspired by radical ideology overseas.”

How much of DHS’s efforts are focused on preventing terrorist attacks based on radical Islamist ideology influenced from abroad, and how much is DHS focused on homegrown, domestic hate groups and anti-government radicals that might also threaten the homeland?

Response: DHS has a number of activities underway to help state, local, tribal and territorial law enforcement and government officials and community groups identify and prevent all forms of domestic terrorism and violent extremism, regardless of the ideology. The goal is to fully integrate CVE awareness into daily law enforcement activities nationwide by building upon existing community oriented policing practices that have proven to be successful for decades. Since the release of the Administration’s national *CVE Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States*, DHS, in coordination with the National Counterterrorism Center (NCTC), Department of Justice (DOJ), the FBI, and State and Local law enforcement, has made progress in the following areas:

1. Better understanding the behaviors and indicators of violent extremism through analysis and research;
2. Supporting law enforcement and community oriented policing efforts through training and grant prioritization; and
3. Enhancing operational partnerships with communities, law enforcement, and international partners.

The Department remains concerned about the consistent level of violent extremism activity, as well as the potential for conflict areas such as Syria to inspire and mobilize US- and Europe-based homegrown violent extremists to participate in or support acts of violence.

We understand that the threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the United States.

Question#:	5
Topic:	homegrown violent extremism
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Moreover, increasingly sophisticated use of the internet, mainstream and social media, and information technology by violent extremists add an additional layer of complexity.

To counter violent extremism (CVE), the Department is working with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to potential terrorist activity within the United States or against U.S. interests abroad, and the best ways to mitigate or prevent that activity.

Our approach to countering violent extremism emphasizes the strength of local communities. We begin with the premise that well-informed and well-equipped families, communities, and local institutions represent the best defense against terrorist ideologies. While our primary purpose is to prevent a terrorist and violent extremist attack by an individual or group recruited by a violent extremist organization, or inspired by a violent extremist ideology, we also support strong and resilient communities as important ends themselves.

Question#:	6
Topic:	major malls in the U.S. 1
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: You state in your testimony that, after the attack on a mall in Nairobi, DHS and FBI have engaged more than 400 major malls in the U.S. in 56 “tabletop exercises.”

Is there, or has there ever been, a similar, credible threat by an armed group large enough to carry out such an attack on a mall in the U.S.?

Response: A recent DHS review of active shooter incidents from 2002 to 2012 involving three or more victims found that at least seven involved individuals targeting shopping malls or centers with small arms. For example, in 2004, an individual was indicted in Columbus, Ohio, for planning to attack an unnamed shopping mall in the local area; he eventually was sentenced to 10 years for conspiracy to provide material support to terrorists.

The attack in Nairobi against the Westgate Mall was carried out by four individuals using small arms and storming tactics—which by their nature can be planned quickly and executed with little to no warning. Commercial facilities, including shopping malls, can be attractive targets due to their ease of access and high numbers of civilians. DHS analysis and communications with our state, local, and private sector partners has focused on the lessons learned in the attack against the Westgate Mall, including the importance of local law enforcement coordination and best practices for securing commercial facilities that are easily accessible to the public, and indicators of possible pre-operational surveillance or planning that terrorist groups or homegrown violent extremists, possibly unknown to law enforcement, could demonstrate were they planning a similar type of attack.

Question#:	7
Topic:	major malls in the U.S. 2
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: You state in your testimony that, after the attack on a mall in Nairobi, DHS and FBI have engaged more than 400 major malls in the U.S. in 56 “tabletop exercises.”

How much did these exercises cost DHS?

Response: There were no discernible incremental costs associated with these exercises. The Department’s engagement in these tabletop exercises involved staffing support rather than direct funding. The National Protection and Programs Directorate’s (NPPD) Protective Security Advisors (PSA) participated in these exercises as part of their ongoing regular support and engagement with other Federal, State and local partners. The Federal Bureau of Investigation led the planning and coordination for the exercises. The exercises were conducted within the PSAs’ local area and thus there were no travel costs.

Question: Is this effort ongoing?

Response: The tabletop exercises are not ongoing. The exercises in 2013 and Spring 2014 culminated in a capstone exercise in August 2014 with Simon Property Group.

Question#:	8
Topic:	tabletop exercises
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: You state in your testimony that, after the attack on a mall in Nairobi, DHS and FBI have engaged more than 400 major malls in the U.S. in 56 “tabletop exercises.”

How much does FEMA spend on hurricane and tornado evacuation drills?

Response: In Fiscal Years 2013-2014, FEMA conducted and/or supported the conduct of 241 natural hazard exercises involving approximately 16,307 participants from 30 states including: Alabama, Alaska, California, Colorado, Florida, Georgia, Hawaii, Idaho, Illinois, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oregon, South Carolina, Texas, Utah, Vermont, Washington, Wisconsin, and Wyoming. The estimated total cost to deliver these exercises was \$22,596,000.

- 71 of the 241 natural hazard exercises focused on hurricane and/or tornado scenarios. Those exercises involved approximately 8,015 participants from 19 states including: Alabama, California, Florida, Georgia, Hawaii, Illinois, Maine, Massachusetts, Michigan, Mississippi, Missouri, Nevada, New Jersey, New York, North Dakota, South Carolina, Texas, Washington, and Wisconsin. The estimated total cost was \$5,649,056.
- 10 of the 71 hurricane and tornado exercises included an evacuation component. Those exercises involved approximately 1,165 participants from nine states and territories including: Alabama, District of Columbia, Florida, Georgia, Illinois, Massachusetts, Minnesota, North Dakota, and South Carolina. The estimated total cost of these exercises was \$750,000. It is important to note that tornado drills emphasize shelter-in-place over evacuation.

In 2013, FEMA also supported the conduct of the Great American Shake-Out Earthquake Drill, which included participation by 22 million people across 43 states and territories.

Question#:	9
Topic:	Unity of Effort initiative
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you discuss the Unity of Effort initiative, and several actions DHS has taken under this initiative, stating:

[t]he actions in this initiative: new senior leader forums led by Secretary and the Deputy, and cross-departmental strategy, requirements, and budget development and acquisition processes that are tied to strategic guidance and informed by joint operational plans and joint operations are building and maturing DHS into one that is greater than the sum of its parts – one that operates much more collaboratively, leverages shared strengths, realizes shared efficiencies, and allows us to further improve our important role as an effective domestic and international partner.

What specific improvements in cross-departmental strategy, requirements, budgeting and acquisitions have been made by this effort?

What shared strengths have been discovered or leveraged and in what capacity?

What specific joint operational plans and joint operations informed these improvements?

What additional collaborations have resulted from this effort?

What efficiencies have been realized as resulted from this effort?

Response: Under Unity of Effort initiative, DHS has improved existing business processes and created new ones where needed, by leveraging shared strengths and emphasizing a more transparent, collaborative approach that better incorporates Component leaders into departmental decision-making processes. In addition,

- The Office of Policy is facilitating a strategic planning effort through the Senior Leaders Council (SLC), which is Chaired by the Secretary, to set the vision and specific, mission-focused outcomes for DHS for the next five years. The SLC includes operational Component leaders, Under Secretaries, and the heads of select other offices. This will ensure that leadership priorities drive DHS planning and investments.
- Planning has commenced on a campaign plan for conducting DHS's Southern Border and Approaches missions. This Component-led planning effort is informed by outcomes and targets, approved by the Secretary. It will not only

Question#:	9
Topic:	Unity of Effort initiative
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

guide DHS joint air, land and maritime operations on the Southern Border and approaches, but it will also identify where DHS has capability gaps that will be analyzed by the new Joint Requirements Council (JRC) and subsequently will inform future resource decisions. This represents a new approach to developing DHS joint operational plans.

- The JRC has been reinstituted and This Component-driven JRC encompasses a program to identify priority gaps and overlaps in Departmental capability needs, provide feasible technical alternatives to meet capability needs, and make recommendations on the creation of joint programs and acquisitions to meet DHS mission needs. The JRC reports directly to the Deputies Management Action Group, which is chaired by the Deputy Secretary.
- The DHS Chief Financial Officer employed an enhanced, unified approach to development of the DHS FY 2016-2020 program and budget submission that enabled leaders to look at the way DHS invests resources – across DHS Component budgets – to better support primary mission areas.
- The Under Secretary for Management (USM) is reviewing the Department’s acquisition oversight framework. In September 2014, USM established formal standards and an appointment process for Component Chief Acquisition Executives (CAEs) to elevate the CAE role and strengthen acquisition oversight.

Unity of Effort leverages successful examples of joint operational activities that exist in seaports such as Charleston, SC, Miami, FL, San Diego, CA and Seattle, WA, and through organizations chartered under the National Interdiction Command and Control Plan such as Joint Interagency Task Force-South in Key West, FL, the El Paso Intelligence Center in El Paso, TX and the Air and Marine Operations Center in Riverside, CA.

In announcing Unity of Effort, the Secretary also cited the Integrated Investment Life Cycle Management (IILCM) pilot study, which tested the linkages between interrelated strategy, capabilities and resources, programming and budgeting, and major acquisition oversight processes. IILCM underscored the need to further strengthen all elements of the process, particularly the upfront development of strategy, planning and joint requirements.

The new Joint Requirements Council has brought under its governance the three portfolios developed during the IILCM pilot. These include vetting and screening,

Question#:	9
Topic:	Unity of Effort initiative
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

cybersecurity, and bio-defense. The JRC is chartering additional portfolio teams in the areas of information sharing and aviation commonality and has expanded the bio-defense portfolio to include Chemical, Biological, Radiation, Nuclear and Explosives (CBRNE). The JRC and these portfolio teams are comprised of members from across DHS, expanding and deepening the cross-component work tested during the IILCM pilot.

Institutionalizing these new processes and procedures is at the forefront of the list of next steps, the goal of which is to enable the effective and efficient conduct of DHS operations and the fulfillment of DHS' missions. In addition, as the thinking of DHS leaders evolves on how best to operate in a joint fashion, DHS will be faced with the need to better understand how to ensure capabilities from across the Department are made available and employed at the right place and time to deal with the Department's steady-state operational needs, as well as during a crisis.

DHS leaders continue to meet with Congressional oversight Committees to discuss plans to enhance efficiency and effectiveness through changes to DHS headquarters elements that conduct strategy, policy and operational functions. The Department also hopes to update its approach to working with homeland security enterprise partners and strengthen the focus on partnering with state and local law enforcement agencies.

These steps are all relatively new, and the Department looks forward to the opportunity further to update Congress as Unity of Effort continues to unfold, including with regard to specific accomplishments.

Question#:	10
Topic:	federal contracts
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The Subcommittee on Financial and Contracting Oversight, which I chair, conducts oversight and investigations of federal spending through contracts and grants. At many agencies, federal contractors sit side by side with federal employees performing similar work. Given the magnitude of spending and the importance of the work performed by federal contractors and grantees, I was surprised to learn that many federal agencies refuse to permit agency witnesses to appear before Congress on the same panel of witnesses as a contractor or grantee. Although there may be legitimate reasons not to do so in certain circumstances, the blanket refusal to allow a federal official and an individual who is being paid by the federal agency the official represents to sit together at a hearing makes it more difficult to conduct efficient and effective oversight. In addition, I believe that this policy no longer accurately reflects the way the federal government does business.

Absent extenuating circumstances, would you agree to testify on the same panel as individuals who receive federal contracts or grants at hearings on the management and oversight of federal spending? If not, please explain why not.

Absent extenuating circumstances, would you agree to make available any employee who reports to you to testify on the same panel as individuals who receive federal contracts or grants at hearings on the management and oversight of federal spending? If not, please explain why not.

Response: Except under extraordinary circumstances, the Department of Homeland Security (DHS) observes the historical practice of not appearing with non-federal witnesses on a single panel. In making its determination, the Department considers whether such appearance would: (1) draw the DHS witness into conflicts that may compromise the legal, commercial or security interests of the United States; (2) introduce subject matter beyond the scope of the hearing or expertise of the witness; and/or (3) undermine the DHS witness' ability to communicate clearly with the Committee.

I am committed to working in strong partnership with your subcommittee in fulfilling its important oversight role and ensuring DHS obtains the best value for the goods and services that support the Department's front-line operations.

Question#:	11
Topic:	rationale for contractors
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The threat to the homeland is ongoing, yet the rationale for contractors is usually to give agencies more flexibility.

How many contractors are employed in the NPPD Office of Cybersecurity and Communications and what is the ratio of contractors to federal employees?

Response: There are approximately 1,800 full- and part-time contractor personnel who contribute to the Office of Cybersecurity and Communications' (CS&C) mission, which equate to 780 full-time equivalent contractors. CS&C has a ratio of 1.01 contractors per each authorized federal position.

Question: Please provide a list of job duties and responsibilities for all contractors employed in the Office of Cybersecurity.

Response: There are a variety of professional types that support the CS&C mission of enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. Among those are software/hardware engineers/analysts, network security specialists/engineers, database analysts, digital forensic analysts, incident response analysts, communications engineers, operations engineers, intelligence/counter-intelligence analysts, public safety engineers, administrative specialists, data management specialists, business operations specialists, control systems security specialists/engineers, help desk specialists, resource managers, acquisitions analysts, program/project managers, procurement specialists, technical writers, policy analysts, and other national/homeland security subject-matter experts. Contractors are selected to perform work rather than Federal employees in the following circumstances, which are outlined in the Department's Balanced Workforce strategy:

1. When they provide specific expertise and/or temporary supplemental support to DHS and its components for services unavailable in the Department; and
2. When they perform functions for which it is neither required nor necessary for federal employees to perform them, and when it is appropriate and cost-effective to do so. Functions that must be performed by Federal employees include:
 - a. Inherently governmental functions;
 - b. Functions closely associated with an inherently governmental function;

Question#:	11
Topic:	rationale for contractors
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

- c. Critical functions that the Department must establish or maintain internal capability to exercise effective control over its mission and operations;
- d. Personal services (except in cases where the Department elects to contract for personal services as authorized by statute); and:
- e. Functions statutorily identified for such consideration.

Question#:	12
Topic:	public awareness
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: You stated during the hearing that September is National Preparedness Month, October is National Cybersecurity Awareness Month, and November is Critical Infrastructure Security and Resilience Month.

What specific efforts does NPPD undertake to make the public aware of these designations?

Response: National Preparedness Month (NPM) efforts are led by the Federal Emergency Management Agency (FEMA), and supported by NPPD. The NPPD communicates to its employees through events and leadership messages about the importance of personal preparedness and steps employees can take to better prepare themselves and their families. NPPD also helps distribute messaging and information to stakeholders to assist in serving as a force multiplier on preparedness messaging.

National Cyber Security Awareness Month (NCSAM) is a collaborative effort with the National Cyber Security Alliance and other public and private partners. NPPD makes the public aware that October is NCSAM through a variety of channels, including participating in an event to kick-off NCSAM and issuing a press release. In addition, the DHS Stop.Think.Connect.™ Campaign works with its partners—which includes 140 government, non-profit, and academic organizations—to notify their stakeholders about NCSAM and encourage them to participate in the month. The NCSAM Partner Packet, which includes information on the NCSAM weekly themes and ways to get involved during the month, was distributed to more than 300 individuals in advance of NCSAM 2014. Throughout NCSAM 2014, there are at least 20 Campaign partners hosting their own in-person events and many others are involved in promoting the month by issuing press releases, posting blogs, updating their website with relevant information, participating in weekly NCSAM Twitter chats, and sharing cybersecurity awareness tips and resources. DHS also works to promote and collaborate on industry involvement in NCSAM through its partnership with the National Cyber Security Alliance.

Promotion has included a presidential proclamation designating October as NCSAM and individual state proclamations to promote the observance of NCSAM among the general public. To further promote NCSAM and online safety, the Campaign is releasing public service announcement videos in October 2014. There are more than 27,000 individuals who receive the monthly Friends of the Campaign newsletter in October, which promotes NCSAM to the general public. The DHS NCSAM website experiences a spike in the number of hits during October. For example, web hits reached 30,592 in October 2013

Question#:	12
Topic:	public awareness
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

compared to approximately 2,000 hits during the other months of the year, which demonstrates the public's interest in NCSAM and the effectiveness of the month's promotion efforts. Finally, NCSAM events held across the country during the month increase public awareness of cybersecurity issues as well as DHS efforts to address the cyber threat.

Critical Infrastructure Security and Resilience (CISR) Month is an annual month-long opportunity to promote, highlight, and educate on the Department of Homeland Security's engagement with our federal and state, local, tribal, and territorial partners and with private sector stakeholders who own and operate the vast majority of our Nation's critical infrastructure. Typically, a presidential proclamation has accompanied an array of communications materials, including talking points and letter templates, and outreach activities. CISR month elevates awareness and encourages dialogue regarding the vital role that critical infrastructure plays in our Nation's well-being and way of life. The month's products and activities also explain why it is important to expand and reinforce critical infrastructure security and resilience.

Question: Who is the target audience for the digital engagement toolkit?

Response: The DHS Stop.Think.Connect. Campaign toolkit is tailored to the needs of various audiences. Toolkit materials are currently available for the following audiences: students, parents and educators, young professionals, older Americans, government, industry, small business, and law enforcement. The toolkit is updating annually to ensure timely and accurate information.

The CISR toolkit is e-mailed to stakeholders or provided upon request. In 2014 the toolkit will be made available on-line and will provide stakeholders and partners with succinct social media messaging, sample blog and news release templates, and other materials instrumental in expanding public awareness.

Question: What were the measurable goals, if any, in creating the toolkit, and how much did it cost?

Response: The DHS Stop.Think.Connect. Campaign toolkit was created to provide tailored information and cyber tips to multiple audiences to help raise cybersecurity awareness among all Americans and empower them to be safer online. Since the toolkit was updated in early 2014, DHS has seen a 61.6 percent average increase in the number of toolkits downloaded per month in 2014 compared to 2013. In addition, the Campaign has distributed 2,495 toolkits in hard copy since January 2014 at an average printing cost of \$1.75 per toolkit. The only non-printing cost associated with toolkits downloaded

Question#:	12
Topic:	public awareness
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

from the website is staff time for the updating/development. The CISR toolkit is created by staff within the NPPD Office of Infrastructure Protection and there are no costs associated with it other than staff resources. NPPD does not print the CISR toolkit, but rather shares it with stakeholders electronically.

The CISR toolkit is one part of a broader CISR Month effort. The two main objectives for CISR Month that are supported by the toolkit are to: (1) elevate awareness and promote dialogue among key audiences regarding the vital role that critical infrastructure plays in our Nation's well-being and way of life; and (2) to highlight why it is important to expand and reinforce critical infrastructure security and resilience.

Question: How many downloads of the toolkit have there been?

Response: Since January 2013, the Stop.Think.Connect. Campaign toolkit has been downloaded from the DHS website more than 9,600 times.

More than 100 CISR month toolkits were requested last year from various sectors. NPPD intends to make the toolkit available for download in 2014.

Question: How many visits to ready.gov have there been during National Preparedness Month as compared to other months?

Response: During National Preparedness Month, there were 17 million page views to ready.gov as compared to the site average of 2.5 million page views each month from January to August.

Question: How many downloads of the Facebook and Twitter header images and profile pictures have occurred this month as compared to other months?

Response: Over the entire month, over 1.4 million people saw the *Ready* Campaign's Facebook content. In addition, the most-downloaded images include: NPM Facebook Header Image: 2,403; NPM Facebook Profile Picture: 1,847; NPM Twitter Header Image: 891; and NPM Twitter Profile Picture: 671. *Ready* does not typically provide header/profile graphics year round for downloading, so there is not a comparable month to month figure for comparison. Over 32,000 Twitter messages used the NPM hashtags, either #NatlPrep or National Preparedness Month.

Question: How much did it cost to produce the Ready Campaign Public Service Announcement?

Question#:	12
Topic:	public awareness
Hearing:	Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Response: For 2014, the *Ready* Campaign worked with The Advertising Council (The Ad Council) to produce general market TV and radio Public Service Announcements in English and Spanish and outdoor/print/web banner PSAs. The Ad Council, as it does with all its clients, seeks free air time from its media sources to air the PSAs. Emergency management partners in twenty states and two geographic areas are co-branding with the Ready Campaign for localized PSAs. In addition, as part of The Ad Council's ongoing relationship with Disney, *Ready* received *Ready Kids* "Big Hero 6" PSAs for TV and radio in English and Spanish and outdoor/print *Ready Kids* PSAs for outdoor/print and web banners. The *Ready*/Ad Council effort for 2014, which cost about \$1.4 million, included the development of the PSAs and related market research, media analysis, campaign tracking and support for a PSA launch event during NPM as well as maintenance, measurement and talent renewal for prior year PSAs. Since its launch in 2003, the *Ready* Campaign has generated nearly \$1 billion in donated media support to encourage Americans to prepare for emergencies.

Additional Background:

Launched in February 2003, the Office of External Affairs *Ready* Campaign is FEMA's national public awareness campaign designed to educate and empower Americans to prepare for and respond to emergencies including natural disasters and potential terrorist attacks. The goal of the Campaign is to get the public involved and ultimately to increase the level of basic preparedness across the nation and more specifically to inform the public about the different types of emergencies that can happen and the appropriate responses. The *Ready* Campaign engages Americans with simple steps to increase the level of basic preparedness across the nation that can ultimately free up valuable response resources when an emergency occurs.

The *Ready* Campaign includes a "general market" effort to reach individuals and families as well as extensions for specific audiences. *Ready Kids* is a tool to help parents and teachers educate children about emergencies and how they can help get their family prepared. *Listo*, *Listo Negocios* and *Listo Ninos* are Spanish language versions of these efforts. The Campaign's messages have been distributed through: television, radio, print, outdoor, and Internet public service advertisements; brochures; www.ready.gov and www.listo.gov web sites; toll-free phone line 1-800-BE-READY; and partnerships with a wide variety of public and private sector organizations.

UNCLASSIFIED//FOUO

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

The Honorable Thomas Carper
Chairman
Committee on Homeland Security and Governmental Affairs
U.S. Senate
Washington, D.C. 20515

DEC 19 2014

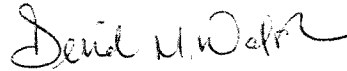
The Honorable Tom Coburn
Ranking Member
Committee on Homeland Security and Governmental Affairs
U.S. Senate
Washington, D.C. 20515

Dear Chairman Carper and Ranking Member Coburn:

(U) Please find enclosed responses to the Questions for the Record from the 10 September 2014 hearing before the Committee on Homeland Security and Governmental Affairs on "Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland."

(U) Please do not hesitate to contact my office at 703-275-2474 if you require further assistance regarding this or any other matter.

Sincerely,



Deirdre M. Walsh
Director of Legislative Affairs

Enclosure:

UNCLASSIFIED when separated from enclosure

Please note:

Responses to some questions have been classified as For Official Use Only (FOUO) and are on file in the committee offices.

Classified By: 2263974
Derived From: ODNI ANA T-12
Declassify On: 20391231

UNCLASSIFIED//FOUO

UNCLASSIFIED/FOR OFFICIAL USE ONLY

Hearing Date: 10 September 2014
 Committee: HSGAC
 Member QFRs: Senator Claire McCaskill
 Witness: NCTC Deputy Director Rasmussen

Questions #1: At the hearing, ISIL's use of social media as a recruitment tool was raised several times. What efforts are being made, if any, to counter ISIL's social media and public relations?

Answer: (U) John Allen, Special Presidential Envoy for the Global Coalition to Counter ISIL, is the lead for all US government efforts, and NCTC is working to support the multi-faceted and diverse efforts being developed to counter ISIL's message. To highlight a number of efforts currently on-going:

- The White House's *Fact Sheet: Strategy to Counter the Islamic State of Iraq and the Levant* describes nine lines of effort necessary to defeat ISIL, including a line of effort focused on exposing ISIL's true nature. In order to address this particular line of effort, NCTC will support the ongoing work being done by the USG to work with our partners throughout the Muslim world to highlight ISIL's hypocrisy and counter its false claim to be acting in the name of religion.
- Working with the Department of State's Under Secretary for Public Diplomacy and Public Affairs, who will lead a whole-of-government effort to degrade ISIL through messaging, NCTC will assist in developing and supporting narratives consistent with the overall strategy of the Coalition.
- The Department of State is working on amplifying statements and videos that undermine ISIL's religious propaganda, e.g. recent condemnations of ISIL from the Grand Mufti of Egypt, the OIC Secretary-General, and the top 150 Muslim leaders throughout Europe and the United States. The Department of State will urge these key voices to form a Muslim world messaging group around the idea that ISIL is anti-Islam.
- The Department of State, working with the Department of Homeland Security, USAID, Center for Strategic Counterterrorism Communications, and other Departments and Agencies, intends to increase the on-the-ground, face-to-face efforts to engage and support influential leaders in countries and communities where ISIL enjoys sympathy and support, to encourage community leaders inside and outside Syria and Iraq to speak out against ISIL, and to expand alumni CVE outreach (over 25,000 alumni in region) whose influence can counter ISIL's message.
- All Departments and Agencies will, as part of their public affairs/public diplomacy efforts, continue to highlight America's \$3 billion in humanitarian aid to Syria and Iraq and our ongoing efforts to mobilize international partners to do more.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Hearing Date: 10 September 2014

Committee: HSGAC

Member QFRs: Senator Claire McCaskill

Witness: NCTC Deputy Director Rasmussen

- The Department of State, Department of Homeland Security, and others are working with the Office of Faith Based and Community Initiatives and the Special Representative to Muslim Communities in support of their innovative efforts to partner with the entertainment industry and Middle East media, including YouTube, Facebook, and Twitter, to increase the creation of counter-ISIL narratives. Already YouTube has confirmed their support to use their media production facilities for rapid response capabilities in response to anti-ISIL messaging. State Department will tap into their network of media executives to garner concrete steps on improving our distribution platforms on anti-ISIL content.

(U) These are just a few of the areas of effort on which the US government is currently working. The approach involves actions both regionally in the Middle East, as well as engaging with our Coalition counterparts. While there is no "quick fix" solution to this challenge, our efforts will build upon the successes listed above and enable each Department and Agency the opportunity to counter the messages of ISIL. As always, each Department and Agency will be engaging with their counterparts throughout the region, and their efforts will be coordinated and synchronized with the National Security Staff, to ensure unity of effort.

Question #2: In your testimony, you express your agreement with the President's remarks and the 9/11 Commission's statement that terrorism poses the greatest threat to the homeland. But terrorism is a tactic that cannot be defeated. Is the threat posed by the tactic itself or specific organizations?

Answer: [REDACTED]

Question #3: The Subcommittee on Financial and Contracting Oversight, which I chair, conducts oversight and investigations of federal spending through contracts and grants. At many agencies, federal contractors sit side by side with federal employees performing similar work. Given the magnitude of spending and the importance of the work performed by federal contractors and grantees, I was surprised to learn that many federal agencies refuse to permit agency witnesses to appear before Congress on the same panel of witnesses as a contractor or grantee. Although there may be legitimate reasons not to do so in certain circumstances, the blanket refusal to allow a federal official and an individual who is being paid by the federal agency the official represents to sit together at a hearing makes it more difficult to conduct efficient and effective oversight. In addition, I believe that this policy no longer accurately reflects the way the federal government does business.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Witness: NCTC Deputy Director Rasmussen

- Answer:**